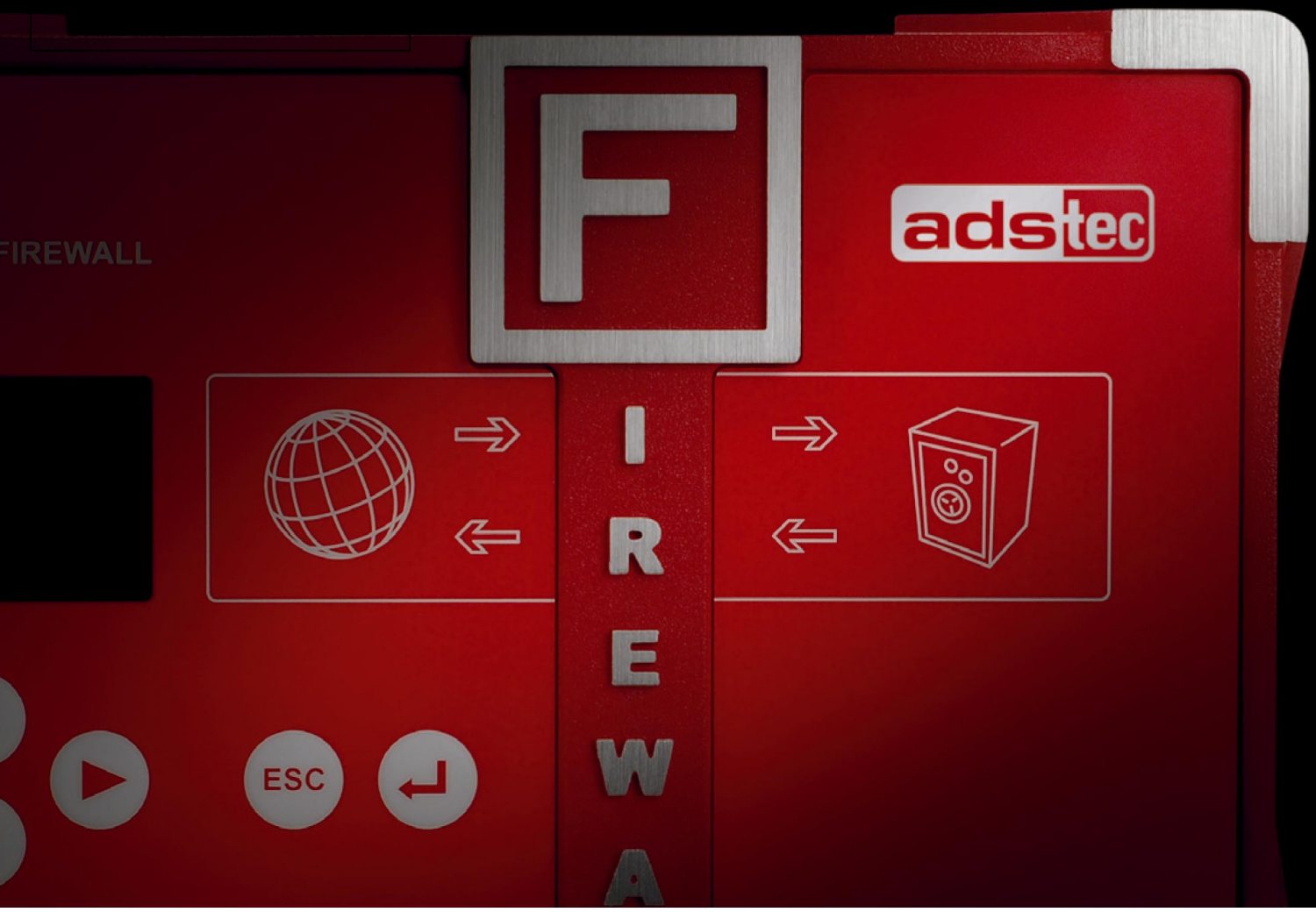
Version 2.2



User Manual

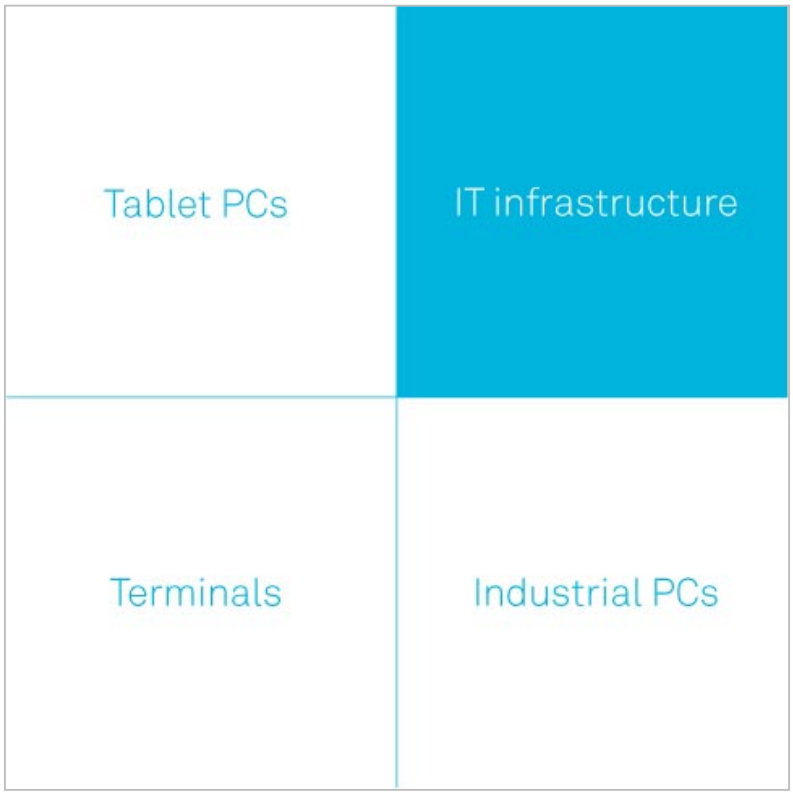
IT Infrastructure

IF1000

adstec

the rugged world of IT®

Product Portfolio



Copyright
© ads-tec GmbH
Raiffeisenstr.14
D-70771 Leinfelden-Echterdingen
Germany

HIGH RISK APPLICATION HAZARD NOTICE

Unless otherwise stated in the product documentation, the device is not provided with error-tolerance capabilities and cannot therefore be deemed as being engineered, manufactured or setup to be compliant for implementation or for resale as an online surveillance device in environments requiring safe, error-free performance, e.g. for implementation in nuclear power plants, aircraft navigation, communication systems, or air traffic control, life saving and military facilities whereby possible device failures might result in death, personal injuries, or serious physical and/or environmental damages (i.e. all applications involving high-risk hazard factors). This is therefore to state that neither ads-tec nor any ads-tec sub-supplier do not hereby undertake any warranty of fitness and/or liability whatsoever, be it by express or by tacit consent, in as far as the suitability of the Firewall to high-risk application hazards is concerned.

INDEX

ABOUT US **6**

1 NOTES **7**

1.1 RELEVANT UNIT DOCUMENTATION 7
1.2 DESCRIPTION OF THE WARNING SYMBOLS USED IN THIS GUIDE 7
1.3 DATA, FIGURES AND MODIFICATIONS 7
1.4 TRADEMARKS 7
1.5 COPYRIGHT 8
1.6 STANDARDS 8

2 OPERATING AND SAFETY INSTRUCTIONS **9**

2.1 SAFETY INSTRUCTIONS 9
2.2 UNIT OPERATION SITE 10
2.3 DAMAGES DUE TO IMPROPER USE 10
2.4 WARRANTY / REPAIRS 10

3 INTRODUCTION **11**

3.1 CUT & STOP 11
3.2 ALARMING 11
3.3 EVENT LOG 11
3.4 DISPLAY /KEYPAD 11
3.5 MANAGED SWITCH 12
3.6 SERVICE 12
3.7 CONFIGURATION VERSIONS 12
3.8 SUPPLY CONTENTS 13
3.9 ENVIRONMENTAL CONDITIONS 13

4 ASSEMBLY **14**

4.1 OVERALL DEVICE DIMENSIONS 14
4.2 ASSEMBLY DIMENSIONS 15
4.3 ASSEMBLY OPTIONS 16
4.3.1 Top hat rail mounting 16
4.3.2 Wall mounting 17

5 SYSTEM FEATURES **18**

5.1 FRONT PANEL OPERATION KEYS 18
5.1.1 IP address and contact names configuration examples 20
5.2 LC-DISPLAY 23
5.3 MENU OVERVIEW – SETTINGS 24
5.3.1 Description of individual menu items 25
5.4 MENU OVERVIEW - STATUS 29
5.4.1 Description of individual menu items 30
5.5 OPERATIONAL LED STATUS DISPLAY 34
5.5.1 Status Display performance upon boot-up process 34
5.5.2 Status Display performance upon reset to default settings 35
5.5.3 Status Display performance upon firmware update 36

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

5.6 INTERFACES 37
5.6.1 24V DC / Backup voltage supply 37
5.6.2 Cut & Alarm 38
5.6.3 LAN-in (RJ45) / PoE (IEEE 802.AF) voltage supply 38
5.6.4 LWL fibre optic 39
5.6.5 COM (RS232) Serial Interface 39
5.6.6 Sim Card Reader compliant to ISO 7816 39
6 INITIAL DEVICE OPERATIONS 40
6.1 FIRST-TIME CONFIGURATION 40
6.2 MANUAL CONFIGURATION OF THE NETWORK ADAPTER 41
6.3 SETTINGS FOR USE WITH INTERNET EXPLORER 8 43
6.4 CALLING UP THE DEVICE WEB INTERFACE 45
7 FIREWALL SETUP ASSISTANT 47
7.1 FIRST-TIME CONFIGURATION WITH THE HELP OF THE SETUP ASSISTANTS 47
7.1.1 Transparent Bridge 48
7.1.2 IP Router 50
7.1.3 Password change 51
7.1.4 Setting activation 52
7.2 SECURENOW! 53
7.3 CONFIGURATION WITH THE HELP OF THE PACKET FILTER 54
7.3.1 Addition of a rule set 54
7.3.2 Changing and searching existing rule sets 55
7.3.3 Pre-configured rule-set upload 56
7.3.4 Definition of a new rule set on bridged Ethernet Interfaces (layer 2) 62
7.3.5 Definition of a new rule set on Standalone IP-Interfaces (layer 3) 75
8 FIREWALL WEB INTERFACE 89
8.1 GENERAL OVERVIEW FOR CONFIGURATION IN THE MENUS 90
8.1.1 IP routing exemplary configuration 90
8.1.2 Error messages 92
8.2 DIAGNOSTICS MAIN MENU ITEM 93
8.2.1 System status 93
8.2.2 Eventlog 95
8.2.3 LAN-in 96
8.2.4 LAN-out 96
8.2.5 Ping test 97
8.2.6 Remote Capture 98
8.3 CONFIGURATION MAIN MENU ITEM 99
8.3.1 IP configuration 99
8.3.2 SECURENOW! 107
8.3.4 Packet filter 108
8.3.5 Cut & Alarm 109
8.3.6 LAN- out 111
8.3.7 Service Modem 111
8.3.8 Basic settings 113
8.3.9 Access control 118
8.3.10 Network 122

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

8.3.11 VPN 133
8.3.12 Utilities 141
8.3.13 Prioritisation 151
8.4 SYSTEM MAIN MENU ITEM 153
8.4.1 Backup settings 153
8.4.2 Software update 155
8.4.3 Factory defaults 157
8.4.4 Save 157
8.4.5 Reboot 158
8.5 INFORMATION MAIN MENU 159
8.5.1 General 159
8.5.2 Technical data 160
8.5.3 Hardware installation 161
8.5.4 Local diagnostics 162
8.5.5 Sitemap 163
9 TECHNICAL DETAILS 164
9.1 DISPLAY DATA 164
9.2 COMPUTER DATA 164
9.3 GENERAL DATA 164
10 SERVICE AND SUPPORT 165
10.1 ADS-TEC SUPPORT 165
10.2 COMPANY ADDRESS 165
11 APPLICATION EXAMPLES 166
11.1 BASIC ROUTER FUNCTIONS 166
11.2 ESTABLISHING AN OPEN VPN CONNECTION 170
11.3 OPENVPN SERVER UNDER WINDOWS 186
11.4 PORT FORWARDING 201
11.5 VIRUS SCAN 208
11.6 SERVICE 214
11.7 SECURENOW! 220
11.8 PACKET FILTER 230
11.9 CERTIFICATES 243
11.10 SCEP 268
11.11 L2TP 273
11.12 IPSEC 282
11.13 MODBUS TCP 302
11.14 IF1000 SERIES MODBUS TCP REGISTER OVERVIEW 305
11.15 SIM CARD 310
11.16 EXTENDED IP ROUTER MODE 312
11.17 REMOTE CAPTURE 316
11.18 1:1 NAT NETWORK MAPPING 320
11.19 PRIORITISATION / SHAPING 329
12 DECLARATION OF CE-CONFORMITY 334

About us



ads-tec GmbH
Raiffeisenstr. 14

D-70771 Leinfelden-Echterdingen
Tel: +49 711 45894-0
Fax: +49 711 45894-990
www.ads-tec.com

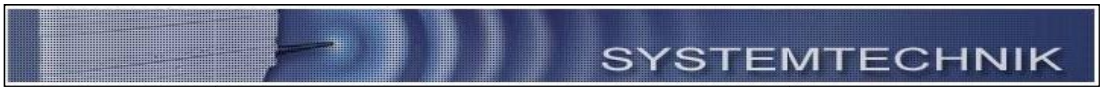
ads-tec GmbH provides large enterprises and globally active corporations with cutting edge technology, up-to-date know-how and comprehensive services in the area of automation technology, data processing technology and systems engineering.



ads-tec GmbH implements full automation solutions from planning to commissioning and is specialized in handling and material handling technologies.



The data systems division develops and produces PC based solutions and offers a broad range of industrial PCs, thin clients and embedded systems.



ads-tec is specialized in modifying and optimizing embedded operating systems and develops software tools to complement its hardware platforms.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

1 Notes

1.1 Relevant Unit Documentation

The following documents are decisive to unit setup and operation:

User Manual

Contains information on assembly, placing into operation and operation of the unit, further to technical data on unit hardware.

Service CD:

Contains the User Manual, the Assembly Guide, the Quick Install Guide and Tools.

1.2 Description of the warning symbols used in this guide



Warning:

The "Warning" symbol precedes warnings on uses or operations that might either lead to personal injury and/or hazards, or to any hardware and software damages.



Note:

This Symbol indicates Notes, terms and/or conditions that strictly need to be observed to ensure optimised and/or zero-defect operations. It also precedes tips and suggestions for efficient unit implementation and software optimisation.

1.3 Data, figures and modifications

All texts, data and figures are non-binding. We reserve the right of modification in accordance with technological progress. At that point in time when the products leave our premises, they comply with all currently applicable legal requirements and regulations. The operator/operating company is independently responsible for compliance with and observance of any subsequently introduced technical innovations and new legal requirements, as well as for all usual obligations of the operator/operating company.

1.4 Trademarks

It is hereby notified that any software and/or hardware trademarks further to any company brand names as mentioned in this User's Guide are all strictly subject to the various trademark, brand name and patent protection rights.

Windows®, Windows® CE are registered trademarks of Microsoft Corp.
Intel®, Pentium®, Atom™ , Core™2 are registered trademarks of Intel Corp.
IBM®, PS/2® and VGA® are registered trademarks of IBM Corp.
CompactFlash™ and CF™ are registered trademarks of SanDisk Corp.
RITTAL® is a registered trademark of the Rittal Werk Rudolf Loh GmbH & Co. KG.

Any further additional trademarks and/or brand names herein, be they domestic or international, are hereby duly acknowledged.

1.5 COPYRIGHT

This User's Guide inclusive of all the images it contains is entirely proprietary and subject to copyright. Any irregular use of this Guide by third parties infringing copyright terms is thus strictly forbidden. Reproduction, translation, as well as electronic and photographic image storage and/or amendment processes, are subject to prior written authorisation directly by M/s. ads-tec GmbH.

Any violation and infringement thereto will be held liable for compensation of all damages.

1.6 STANDARDS

This unit is compliant with the provisions and safety objectives of the following EU Directives:

- This unit is compliant with the CE mark testing specification limits as defined in the European test standards EN 55022 and EN 50082-2
- This unit is compliant to the DIN EN 60950 (VDE0805, IEC950) testing specification limits on "Safety of Information Technology Equipment"
- This unit is compliant to the DIN EN 60068-2-6 (sinusoidal vibration) testing specification limits
- This unit is compliant to the DIN EN 60068-2-27 (shock and bump) testing specification limits
- The device has a UL-Certification regarding UL-508 and is listed under the UL-File-Nr. E305773, Section 2



Note:

A corresponding declaration of conformity is available for competent authorities, care of the Manufacturer. Said declaration can be viewed at all times upon request.

For full compliance to the legal requirements in force on electromagnetic compatibility, all components and cables used for unit connection must also be compliant with said regulations. It is therefore necessary to employ BUS and LAN cables featuring screened plug connectors, to be strictly installed as per the instructions contained in the User Manual.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

2 Operating and Safety Instructions

The unit operates under electrical tension and implements supersensitive component parts. Intervention by the User is required only for power supply line connection operations. Should any further alterations be required, it is necessary to consult either with the Manufacturer directly or with authorised service personnel accordingly. During said connection operations, the unit must be completely powered down. Specific requirements need to be met concerning the prevention of electrostatic discharge on component construction parts during contact. If the unit is opened up by a non authorised individual, the User may be subject to potential hazards and, warranty conditions are terminated.

General Instructions:

- This User's Guide must be read and understood by all User's and must be available for consultation at all times
- Assembly, operation start-up and unit operation must only be conducted by appropriately qualified and trained personnel
- All individuals and operators using the unit must strictly observe all safety and use instructions as provided within the User's Guide
- All regulations and prescriptions on accident prevention and safety in force c/o the unit installation site must be strictly observed at all times
- This User's Guide provides all the most important directions as required for safe and security oriented operation
- Safe and optimised unit operations are subject to appropriate storage, proper transport and handling, accurate unit setup, start-up and operation

Note:

Only the ads-tec original firmware / software is allowed for any of the adjustments and features described in this User's Guide. Deployment of any firmware / software that has not been released by ads-tec will terminate all warranty conditions.

2.1 Safety Instructions

Warning:

For the prevention of possible unit damages, all cable lines (power supply, interface cables) must be hooked up strictly with the unit in power-OFF conditions.

Warning:

All unit assembly operations must be strictly conducted only under safe, secure and zero-potential conditions.

Note:

When handling parts and components susceptible to electrical discharge, please accurately observe all the relevant safety provisions.

(DIN EN 61340-5-1 / DIN EN 61340-5-2)



2.2 UNIT OPERATION SITE

This unit is engineered for industrial application. It is necessary to ensure that specified environmental conditions are maintained at all times. Unit implementation in non specified surroundings, i.e. onboard ships, in explosive atmospheres or at extreme heights, is prohibited.



Warning:

For the prevention of water condensate accumulation, the unit should be turned ON only when it reaches ambient temperature. This is also particularly necessary when the unit is subject to extreme temperature fluctuations and/or variations.

Avoid overheating during unit operations: the unit must not be subject to direct sunlight or to any other direct light source.

2.3 DAMAGES DUE TO IMPROPER USE

Should the service system have evident signs of damages incurred e.g. due to wrong operation or storage conditions or due to improper unit use, the unit must be decommissioned or scrapped. Ensure that it is safe from accidental re-implementation.

2.4 WARRANTY / REPAIRS

During the unit warranty period, any repairs thereto must strictly be conducted solely by the manufacturer or by service personnel that has been duly authorised by the manufacturer.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

3 Introduction

The Industrial Firewall constitutes a link between the IT world and automation, thereby meeting the requirements of IT security as well as those by the production line maintenance personnel. It enables monitoring and control of the plant setup network, and of the relative access points. Its essential security protection mechanism is constituted by the event-dependent and physical network separation. This Firewall furthermore offers, amongst others, a secure access in the event of service operations; it enables traffic shaping and is capable of implementing the available virus scanners.



Note:

*For the efficient online configuration of your ads-tec devices, it is possible to download the current version of the free tool „**IDA light**" on the company`s homepage **http://www.ads-tec.de**. The tool offers you for example the possibility of defining individual parameters or whole groups of parameters at a Server device and to transfer your settings to a limited selection and/or to all ads-tec devices of same design and version, without having to make these configurations time-consuming at each individual device. You also have the possibility of assigning sequential IP addresses for your ads-tec devices.*
With IDA light you can comfortably provide own groups of parameters according to your specific requirements and modify them at any time.

3.1 Cut & Stop

During critical start-up or production phases, the Ethernet uplink can be physically disconnected i.e. via hardware, through a 24 V input. This will safely rule out both intentional and unintentional external manipulation.

The uplink is reconnected through the same input. This function makes integration into an automation concept very simple.

3.2 Alarming

In the event that a rule is violated, the alarm signal is reported to the control centre through an output. Necessary measures can be automated directly. For example, acoustic indicator lights can signal the alarm condition.

E-mails can be sent out automatically to signal a rules violation event.

3.3 Event log

A zero-voltage event logbook with retentive memory stores all events whenever the firewall is disconnected from the power supply (NV-RAM option).

The event logbook can be read out either locally or via a central Syslog server.

3.4 Display /Keypad

The built-in display can be used to configure the essential unit functions.It is thus possible to obtain a quick system analysis, e.g. of the network load, directly from the display.

The display and keys can be password-protected against unauthorized manipulation.

3.5 MANAGED SWITCH

Network segments can be set up without any additional hardware by using the managed switch integrated into the firewall. It is possible to connect multiple systems or terminals up to one Firewall.

Each port can be switched off individually to prevent unauthorized data traffic monitoring.

3.6 SERVICE

Service access via a secure service port.

Connecting the Firewall to an analogue, ISDN or GPRS modem for dial-in access provides for affordable remote maintenance, even without an Internet connection.

3.7 CONFIGURATION VERSIONS

The device is available in 4 configuration versions:

Configuration Version	LAN-in	LAN-out	NVRAM
IF 1100	**RJ45**	**RJ45**	**-**
IF 1110	**RJ45**	**RJ45**	**yes**
IF 1200	**LWL**	**RJ45**	**-**
IF 1210	**LWL**	**RJ45**	**yes**

RJ45 (Registered Jack 45 = standardized jack) provided per an Ethernet standard as frequently implemented in telecom applications. The transmission method is equivalent to 10/100Mbits half and full DUPLEX 100 BASE-TX.

LWL (fibre optic connection) are flexible optic media for controlled conduction of light. Contrarily to the Ethernet standard, the fibre optic connection technology is insensitive to voltage interference.

The plugs required for implementation are equivalent to the MTRJ Standard Multimode with a 100Base-FX 100 Mbit/s Ethernet transmission method via fibre optics.

NVRAM (non-volatile RAM = non-volatile Random Access Memory) is an electronic memory storage technology whereby data is stored even without maintenance of power supply.



Note:

The LAN-in interface can be equipped with an RJ45 or with an LWL fibre optic connection, as the case may be.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

3.8 Supply Contents

Please check supply package contents for integrity and completeness:

- 1 device
- 2 x two-pole COMBICON plugs
  Manufacturer: Phoenix Contact
  Item description/item short text: FMC 1.5 / 2-STF-3.5
- 1 x four-pole COMBICON plug
  Manufacturer: Phoenix Contact
  Item description/item short text: FK-MCP 1.5 / 4-STF-3.81
- 1 m Ethernet cable
- Quick Install Guide / Quick Assembly Guide
- GNU General Public License
- Service CD

3.9 Environmental Conditions

The unit can be put into operation and used under the following conditions. Failure to observe any one of the specified data will immediately terminate all warranty conditions. ads-tec cannot be held liable for any damages arising due to improper device or unit use and handling.

- Permissible ambient temperature

during operation	from 5 to 60°C
during operation (UL)	from 5 to 50°C
during storage	from -20 to 50°C

- Humidity

during operation	10 to 85%, without condensate
during storage	10 to 85%, without condensate

- Vibration

during operation	1 G, 10 to 500 Hz (DIN EN 60068-2-6)

- Shock

during operation	5 G, with a 30 ms half-cycle (DIN EN 60068-2-29)

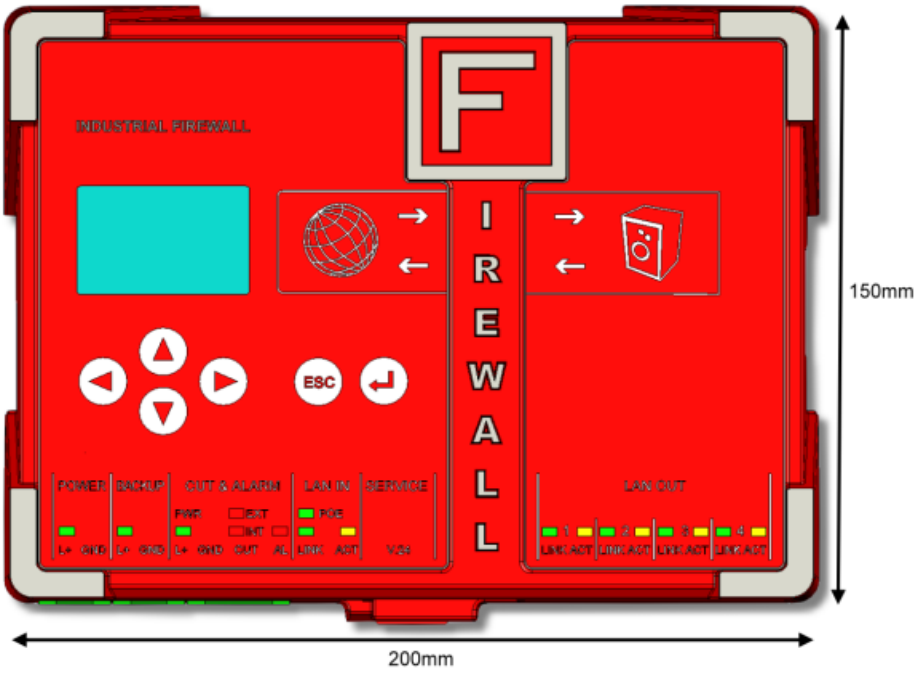


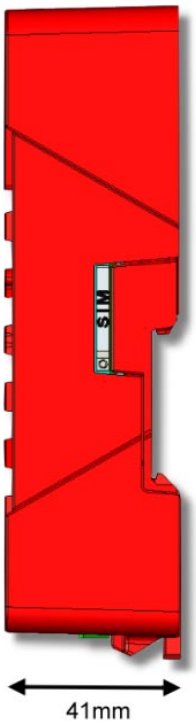
Note:
For Use In Pollution Degree 2 Environment Only Type 1 "indoor use only".

4 Assembly

4.1 Overall Device Dimensions

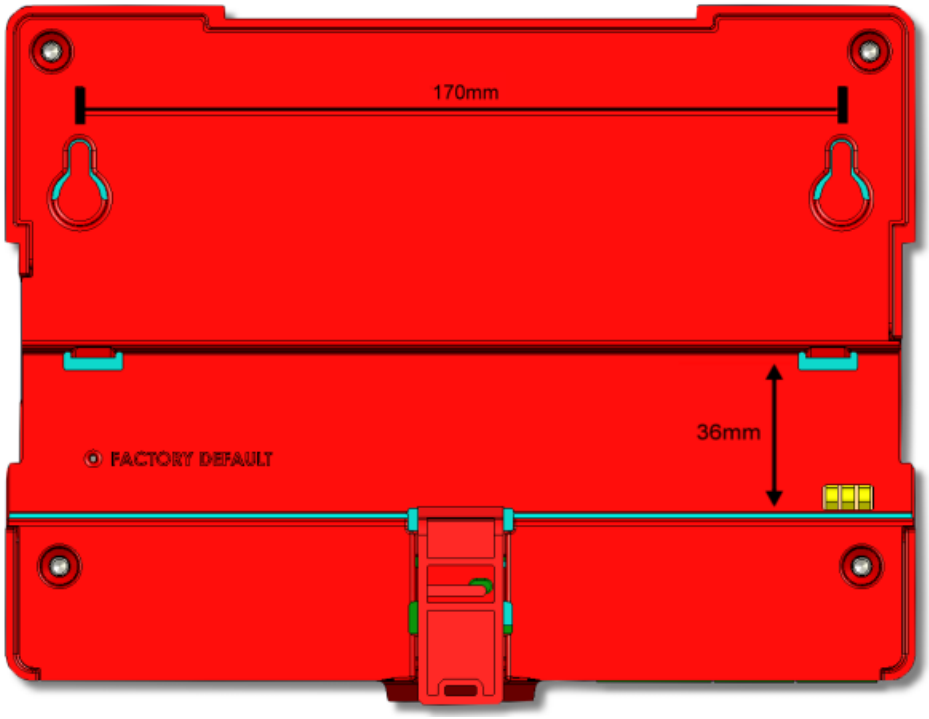
Height: 150mm
Width: 200mm
Depth: 41mm





© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

4.2 Assembly Dimensions

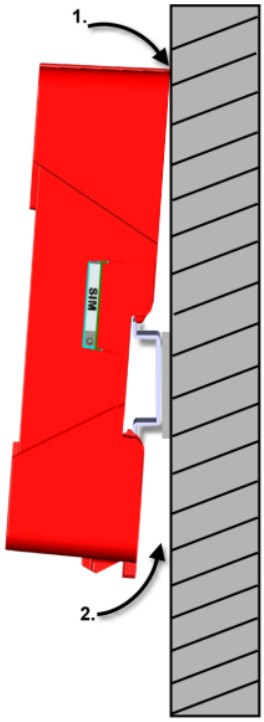


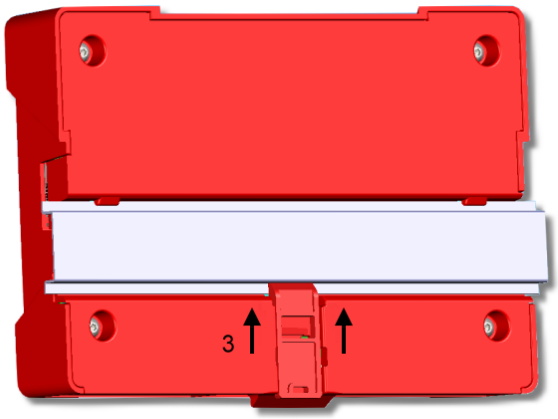
4.3 Assembly Options

The device unit is designed for both top hat rail mounting as well as for wall-mounting.

4.3.1 Top hat rail mounting

1. The Firewall must be placed obliquely up against the top of the top hat rail.
2. Fix it on by pressing the underside lightly up against the rail.
3. The Firewall must firmly snap into place on the top hat rail.





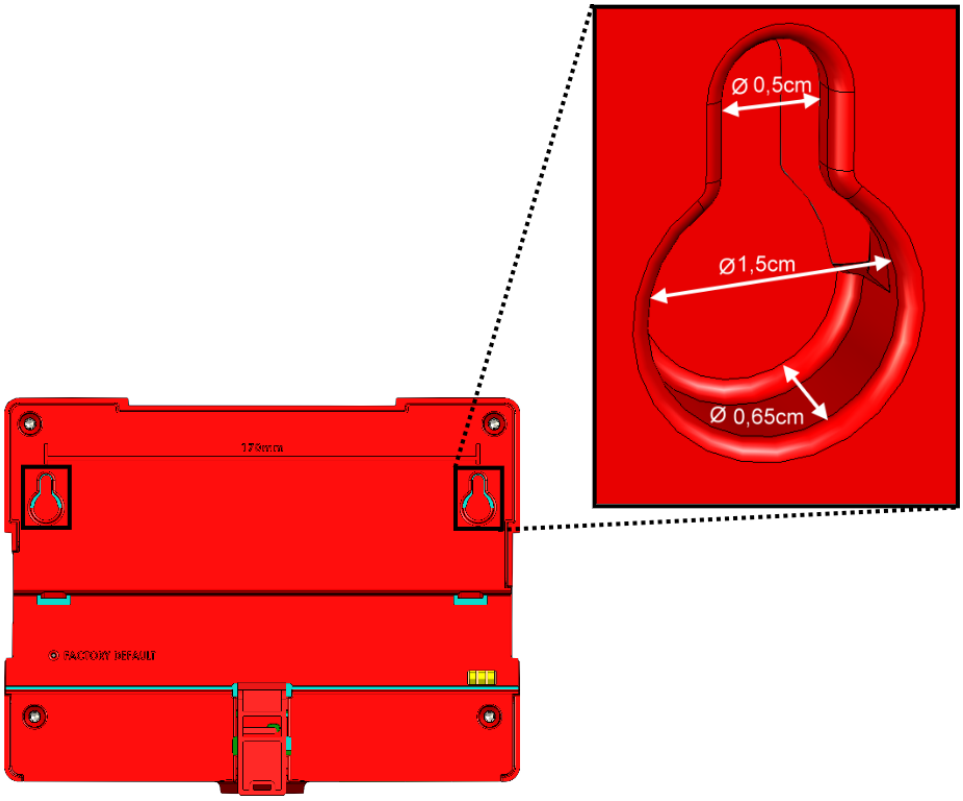
Note:
Check to make sure that the Firewall will not detach itself from the top hat rail by lightly tugging the underside forward.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

4.3.2 WALL MOUNTING

1. Provide for screws on the relative device mounting wall so that they are set horizontally level, with a distance between screws amounting to 170mm.

2. Attach on the Firewall by way of the appropriate cavities as illustrated.



5 System Features

5.1 Front Panel Operation Keys

The device is provided with operation keys for navigation and unit configuration via the LCD menus. Said LCD menus are easily accessed via simple operation of the **ESC** or the **ENTER** keys. You will find a description of the single menu items in the following LC display section.

The front panel operation keys are provided with the following functions:

Symbol	Navigation function	Configuration Function
	Press to exit the current menu level. (**ESC**)	If the input mode is activated, the variation can be overruled/abandoned by pressing **ESC**.
	Press to access a menu level or to confirm a change entry. (**ENTER**)	To enter or to change data, the input mode must first be activated by pressing **ENTER**. This will have only one digit flashing. To adopt the change entries, the input mode must first be deactivated by pressing **ENTER**. This will highlight the whole line. For selection amongst a number of options, selection is activated via this key. selection of either German or English from the available language options).
	Menu navigation direction arrow (**UP**)	For selection amongst a number of options, the **UP** key will access and highlight the selection item in ascending/up order (e.g. selection of either German or English from the available language options). Upon entry or change of various data, the highlighted digit can be accessed and changed in ascending/up direction. The succession of the characters is provided in the ASCII code. However, a space character is assigned for simplification of first-time operation of the **DOWN** navigation direction option. If the key is pressed a second time, the system proceeds with ASCII character strings.

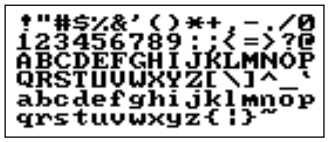
© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

	Menu navigation direction arrow (**LEFT**)	If the input mode is activated, each digit is marked and can be changed via access with the **UP** and **DOWN** arrow keys.
	Menu navigation direction arrow (**DOWN**)	For selection amongst a number of options, the **DOWN** key will access and highlight the selection item in ascending/up order (e.g. selection of either German or English from the available language options). Upon entry or change of various data, the highlighted digit can be accessed and changed in ascending/up direction. The succession of the characters is provided in the ASCII code. However, a space character is assigned for simplification of first-time operation of the **DOWN** navigation direction option. If the key is pressed a second time, the system proceeds with ASCII character strings.
	Menu navigation direction arrow (**RIGHT**)	If the input mode is activated, each digit is marked and can be changed via access with the **UP** and **DOWN** arrow keys.



Note:

To carry out changes in the LCD menus, the following character set is available.

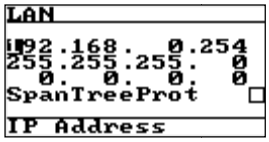
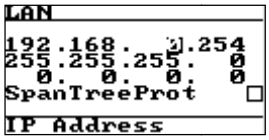
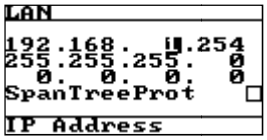
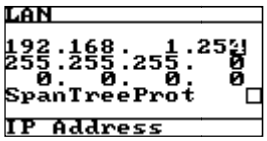
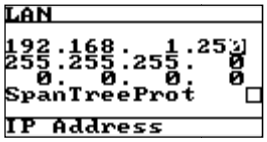
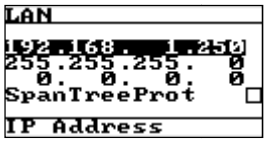
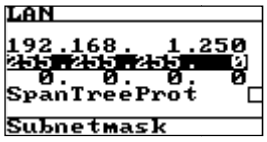
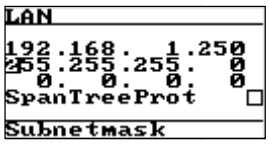


5.1.1 IP ADDRESS AND CONTACT NAMES CONFIGURATION EXAMPLES

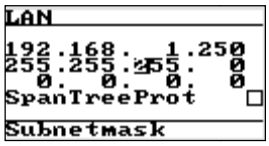
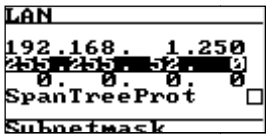
IP Address

Default IP address 192.168.0.254 needs to be changed into 192.168.1.250 whilst the subnet mask must be changed from 255.255.255.0 into 255.255.52.0.

The IP address is highlighted and the input window is deactivated. To change the IP, proceed as follows:

Menu		Action
		Press **ENTER** to activate the iput mode. -> The input focus will be active on the first digit.
		Press the **RIGHT** direction arrow key eight times -> The input focus will be active on the **0**
		Press the **UP** direction arrow key once. -> Change to **1**
		Press the **RIGHT** direction arrow key three times -> The input focus will be active on the **4**
		Press the **DOWN** direction arrow key four times -> Change to **0**
		Now press **ENTER** to confirm all the changes to the first line in the input mode. -> The overall IP is highlighted The text message "Please wait" will come up on display whilst the data is being stored. If the input mode is exited by pressing ESC, the changes are overruled/ abandoned.
		Press the **DOWN** direction arrow key once -> The subnet mask is highlighted
		Press **ENTER** to activate the iput mode. -> The input focus will be active on the first digit.

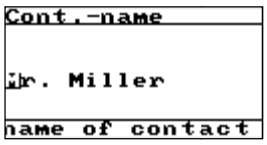
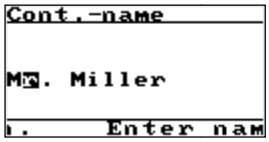
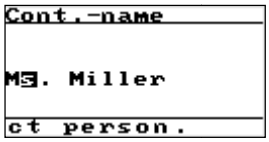
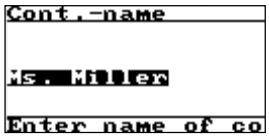
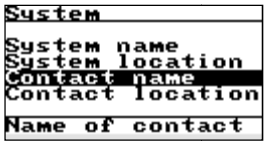
© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

		Press the **RIGHT** direction arrow key six times -> The input focus will be active on the **2**
		Press the **DOWN** direction arrow key twice -> Change on the space
		Press the **RIGHT** direction arrow key twice -> The input focus will be active on the **5**
		Press the **DOWN** direction arrow key three times -> Change to **2**
		Now press **ENTER** to confirm all the changes to the first line in the input mode. -> The overall IP is highlighted The text message "Please wait" will come up on display whilst the data is being stored. If the input mode is exited by pressing ESC, the changes are overruled/ abandoned.
		Press the **ESC** key to exit this menu. All the changes entered have been duly stored.

CONTACT NAME

Contact name Mr. Miller must be changed to Ms. Miller.

The Contact Name is highlighted and the input window is deactivated. To change the Contact Name, following steps are required:

Menu		Action
		Press **ENTER** to activate the iput mode. -> The input focus will be active on the first digit.
		Press the **RIGHT** direction arrow key once. -> The input focus will be active on the **r**
		Press the **UP** direction arrow key once. -> Change to **s**
		Now press **ENTER** to confirm all the changes to the first line in the input mode. -> The overall Contact Name is highlighted The text message "Please wait" will come up on display whilst the data is being stored. If the input mode is exited by pressing ESC, the changes are overruled/ abandoned.
		Press the **ESC** key to exit this menu. All the changes entered have been duly stored.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

5.2 LC-DISPLAY

The device is fitted with an LCD which allows direct access to configuration settings. Any modifications to the firewall and web interface settings made via the LCD menu will take effect immediately. Furthermore, the display shows event messages and status information for quick on-site system analysis.

The LCD menu option **Lock** can be used to lock the display and all front panel keys. When these are locked, the device **PIN** is required to access and/or modify any device information. Hence, the **Lock** function protects the device against unauthorised on-site modifications.

The LCD menu can be accessed by pressing the **ESC** or **ENTER** key.

The LCD menu contains the following main menu items:

SETTINGS

Allows configuration of basic Firewall settings, which includes locking the display and all front panel keys. Also allows setting the local IP address as well as the display language and various system information.

STATUS

Shows all current event log entries and device information. Also allows initiating a self test of the following components: display, front panel keys, CUT and ALARM function.The connection control displays the state of the Service, Open VPN and IPsec connections.

Note:

The default language setting is English. In order to select a different language, open the main menu and select the following menu items:

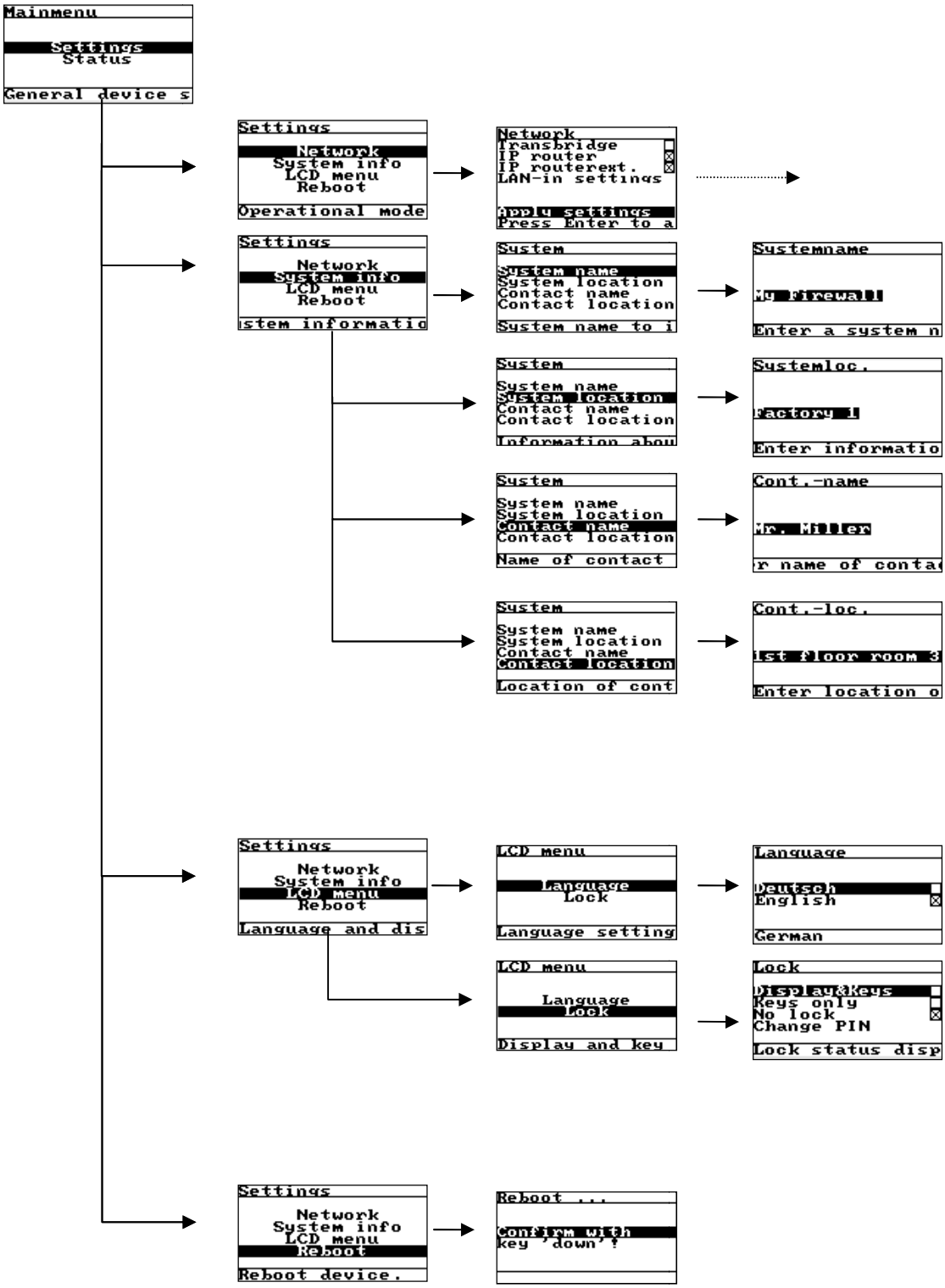
Settings/ LCD menu/ Language

*Confirm your selection by pressing **ENTER**.*

(Selection will be marked by an X.)

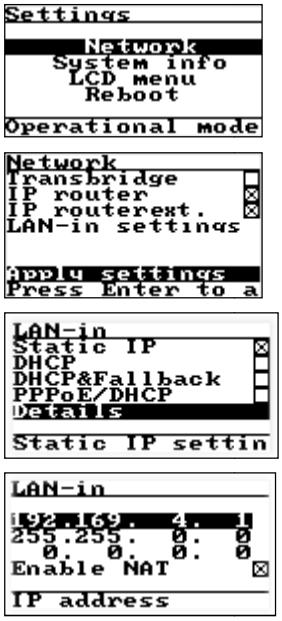
*Then leave the menu by pressing **ESC**.*

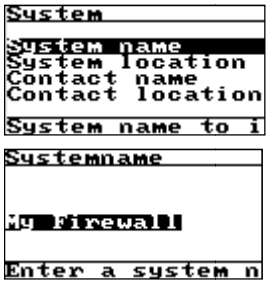
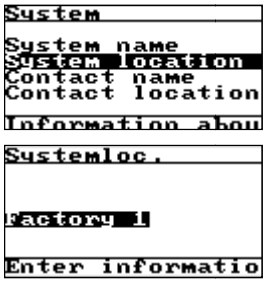
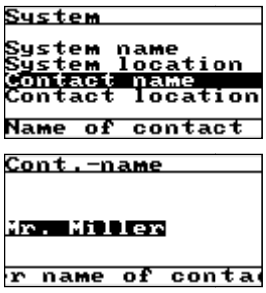
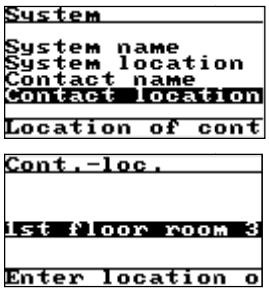
5.3 MENU OVERVIEW – SETTINGS



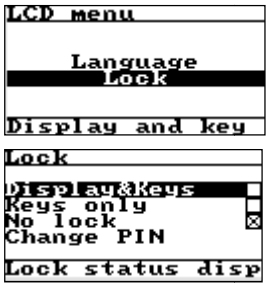
© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

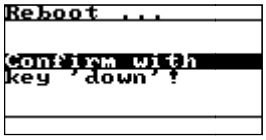
5.3.1 DESCRIPTION OF INDIVIDUAL MENU ITEMS

Network		
Display	**Selection**	**Description and Notes**
Network		
	**Transbridge**	The network mask allows setting the operational mode. Additional options are available for each mode. In Transparent Bridge mode, the Firewall acts as a Layer 2 Bridge and is invisible to all participants. Transbridge= LAN Settings
	IP Router	The Firewall treats the networks at the LAN-In and LAN-Out interfaces as two separate networks and filters these separately. Hence, this mode requires that two independent IP addresses be configured for LAN-In and LAN-Out. IP-Router = LAN-In/LAN-Out Settings.
	LAN Settings	Depending on the selected operational mode, IP address assignment can be configured under LAN Settings. Available options are: Static IP address, DHCP, DHCP fallback and PPPoE/DHCP.

System Info		
Display	**Selection**	**Description and Notes**
System name		
	**System name**	This name serves as a unique identifier of the device at its installation site. The Firewall system name displayed can be specified/changed here. You may freely choose a Firewall system name. The name entered here will be shown in the LCD menu and in the web interface.
System location		
	**System location**	This item serves as a unique identifier of the location at which the device is operated. The Firewall system location can be specified/changed here. You may freely choose a Firewall system location. Specifying the system location provides additional information on the device location. The location entered here will be shown in the LCD menu and in the web interface.
Contact name		
	**Contact name**	This item serves as a unique identifier of the responsible contact person. A contact name can be specified/changed here. You may specify a contact person that can be contacted in case problems occur or maintenance is required.
Contact location		
	**Contact location**	This item serves as a unique identifier of the responsible contact person and their location. A contact location can be specified/changed here. In addition to the name of the contact person, you may also specify their location.

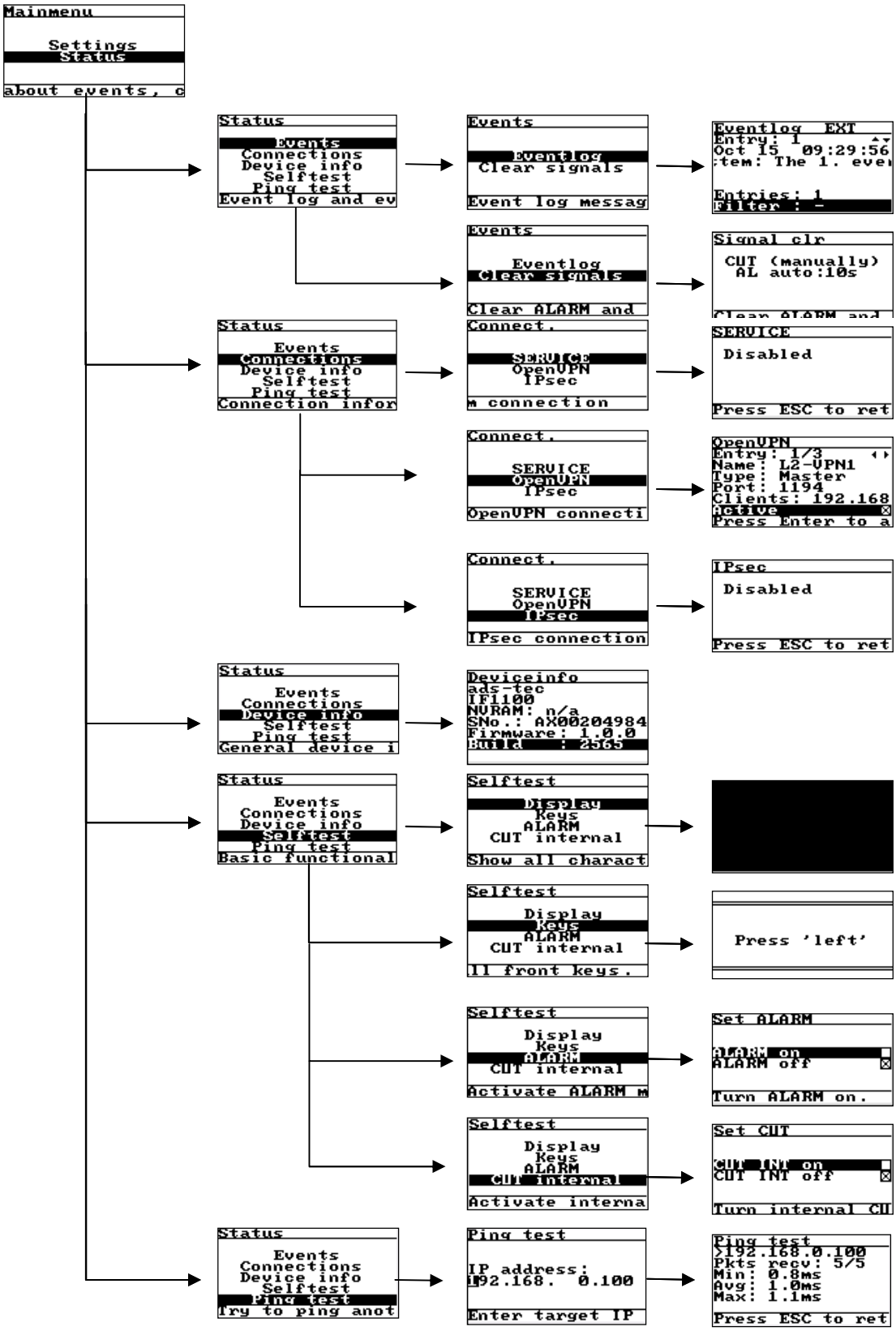
© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

LCD Menu		
Display	**Selection**	**Description and Notes**
Language		
	**German** **English**	Two language options are available. Changing the language setting here will also affect the language of the web interface. The default setting is English.
Display	**Selection**	**Description and Notes**
Lock 	**Display & Keys**	The display and keys can be locked to prevent unauthorised access. When locked, the display will not show any information and the keys can no longer be used to modify the device configuration. The only operation possible in locked mode is entering the required **PIN** for unlocking the display and keys. The lock will only become active once the user exits the LCD menu by pressing **ESC**. The **PIN** needs to be entered correctly in order for all LCD menu functions to become accessible again. When the Firewall is turned off and on again, the lock will still be active and the **PIN** needs to be re-entered.
	Keys only	This option allows locking the keys separately from the display. With locked keys, the LCD menu can no longer be used to modify the device configuration. The LC display will, however, still show current network load and other system information. The only operation possible in locked mode is entering the required **PIN** for unlocking the display and keys. The lock will only become active once the user exits the LCD menu by pressing **ESC**. The **PIN** needs to be entered correctly in order for all LCD menu functions to become accessible again. When the Firewall is turned off and on again, the lock will still be active and the **PIN** needs to be re-entered.

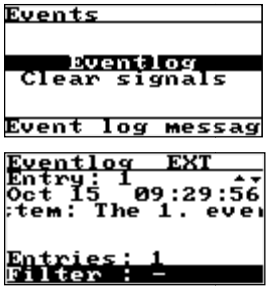
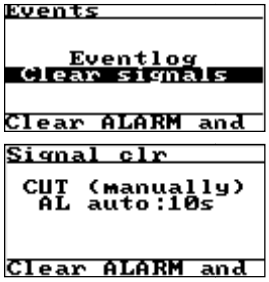
	Unlocked	By default, neither keys nor display are locked.
Change PIN		
	**new PIN**	In order to change the **PIN**, the old PIN needs to be entered. The **PIN** may be changed independently from the web interface password. The default **PIN** is empty; any user-defined **PIN** may be up to 14 digits long.
Reboot		
Display	**Selection**	**Description and Notes**
 		The reboot option allows re-starting the Firewall via the LCD menu. Confirm selection of this option by pressing the down key ▼.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

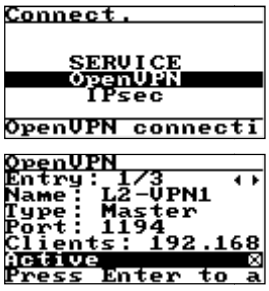
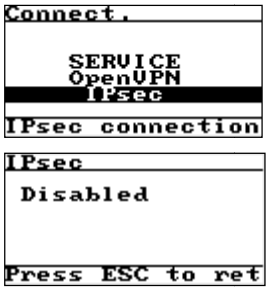
5.4 MENU OVERVIEW - STATUS



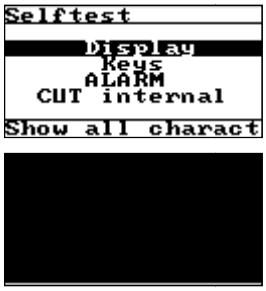
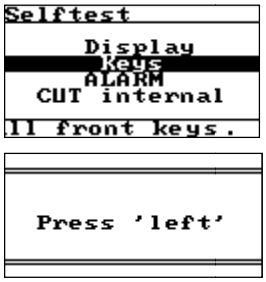
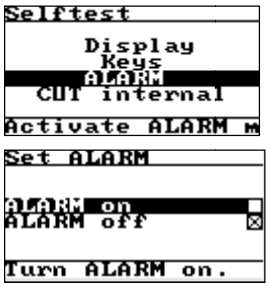
5.4.1 DESCRIPTION OF INDIVIDUAL MENU ITEMS

Events		
Display	**Selection**	**Description and Notes**
Event log		
	**Event log**	The event log allows retracing system messages and alarms. Select individual log entries using the **UP** and **DOWN** keys. The event log display is comparable to a transcript of messages. Use the Event log menu to view any logged events.
Message Ack.		
	**Message Ack.**	Use the Message Acknowledgement option to override or end, respectively, any events logged in the event log. Manually acknowledging event messages will end all active events. In automatic setting, events will be acknowledged automatically after a predefined period of time.

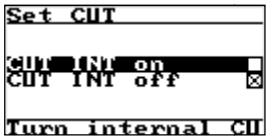
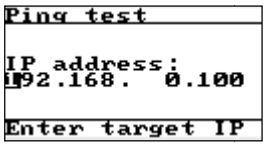
© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

Connections		
Display	**Selection**	**Description and Notes**
Service		
	**Service**	Use the menu item Service to check or monitor, respectively, the status of a service connection. If the device is successfully connected, the state changes to connected. If the device is not properly connected, the state shows diconnected.
Open VPN		
	**OpenVPN**	Use the menu item OpenVPN to display all active VPN connections. Settings can be changed directly via the LCD menu.
IPsec		
	**IPsec**	Use the menu item IPsec to display all IPsec-related information and settings. The display screen can be used to monitor the IPsec status. Settings can be changed directly via the LCD menu.

Device Info		
Display	**Selection**	**Description and Notes**
Device Info		
	**Device Info**	This option displays general device information. The screen shows the name of the manufacturer, the device variant, whether a NVRAM card is installed, the current firmware version, and the current firmware build.

Device Test		
Display	**Selection**	**Description and Notes**
Display		
	**Screen**	Starts the display test. Press **Enter** to start the display test. Perform this test to check the display for correct functioning. You can visually check whether all characters are displayed properly on the display. Four different test screens will appear, each of which will need to be confirmed by pressing any front panel key. When the test is finished, you will automatically be taken back to the menu view.
Keys		
	**Keys**	Starts the key test. Press **Enter** to start the key test. Perform this test to check the keys for correct functioning. You will be prompted to press specific keys, whereupon you should press the respective key. In case one key is defective, you may exit the test using the other keys. When the test is finished, you will automatically be taken back to the menu view.
ALARM		
	**Alarm**	Sets the alarm output. Sets the alarm output and turns on the alarm LED. The letters **AL** will appear in the upper right corner of the display, indicating that an alarm was triggered. **AL** will continue to flash until the alarm is either switched off or acknowledged automatically. Perform this test to check the alarm output for correct functioning.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

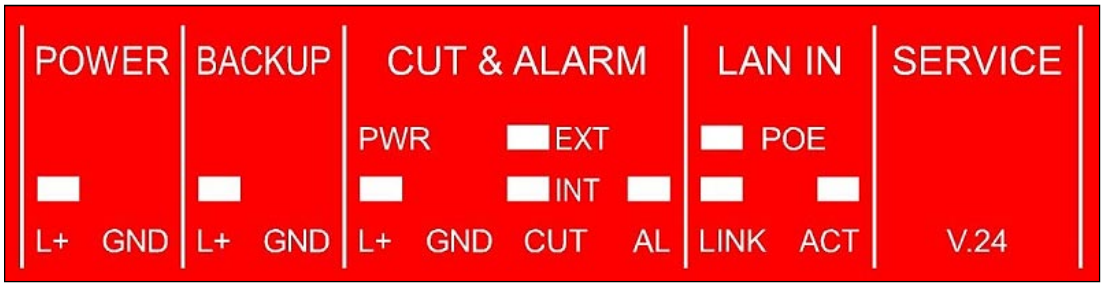
Internal CUT		
 	**Internal CUT**	Sets the internal CUT. Sets the CUT and turns on the CUT LED. The letters **INT** will appear in the upper right corner of the display, indicating that an internal CUT was triggered. **INT** will continue to flash until the internal CUT is either switched off or acknowledged automatically. Perform this test to check the internal CUT for correct functioning.
Ping-Test		
Display	**Selection**	**Description & Notes**
Ping-Test  	**Ping-Test**	With the aid of the PING-Test, the accessibility of an affiliated remote station is tested. The PING-Test sends an echo request packet to the destination address of the remote station to be tested and then proceeds with test information assessment. Enter the destination address that needs to be tested in IP address form in the appropriate entry field. It is furthermore necessary to enter the packet quantity required to be sent. Said quantity is limited to a maximum of 10 packets.

5.5 Operational LED Status Display

5.5.1 Status Display performance upon boot-up process

Te boot-up process starts as soon as the firewall is supplied with a voltage source. With the aid of the Lan-in LEDs it is possible to check whether the Firewall is booting up as well. The table herunder provides boot-up process LED blink frequency via which it is possible to check that the device is booting up correctly. In the example, no LAN-in cable / PoE is connected up.

The minute the traffic display comes up on the LCD, the boot up process has been successfully concluded.



POWER	SIGNAL	ACTION
L+	■	The device is provided with voltage via POWER and is ready for operation.
BACKUP		
L+	■	The device is provided with BACKUP voltage supply and is ready for operation.
LAN IN		
LINK / ACT	◧ ◨	The LEDs flash briefly just once
	□ □	The LEDs are off
	◧ ◨	The LEDs flash briefly just once
	□ □	The LEDs are off
LINK	◧	The LED blinks at regular intervals
LINK / ACT	◧ ◨	The LEDs flash briefly just once
	□ □	The LEDs are off
	◧ ◨	The LEDs flash rapidly.
	□ ◨	The LEFT LED goes off / the ACT led goes on blinking
ACT	◨	The LED flashes rapidly
	□	The LED is off
The traffic display is shown up on the LCD.		

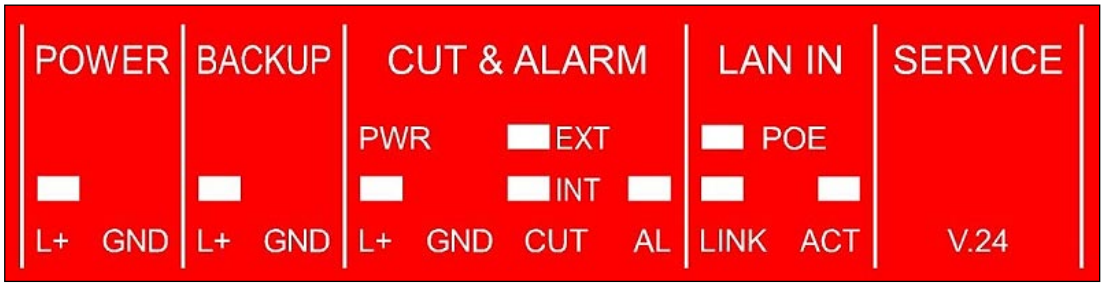
© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

5.5.2 STATUS DISPLAY PERFORMANCE UPON RESET TO DEFAULT SETTINGS

Via the **Factory Default** keys on the rear side of the Firewall it is possible to reset the Firewall back to its default factory settings at any time, independently of its configuration.

To set the Firewall back to its default settings, the factory default keys must be pressed during current operations. In the example, no **LAN-in** cable / PoE is connected up.

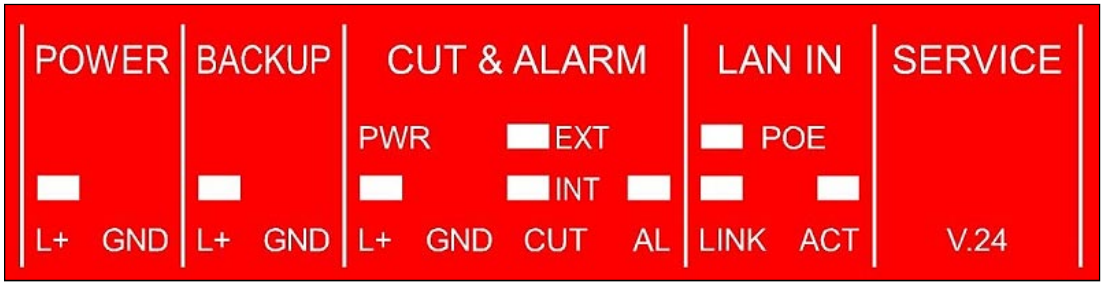
The factory default keys must be pressed once, briefly in order to start the set-back to default settings process. The table herunder provides boot-up process LED blink frequency via which it is possible to check that the set-back to default settings process is being run correctly.



POWER	SIGNAL	ACTION
L+		The device is provided with voltage via POWER and is ready for operation.
BACKUP		
L+		The device is provided with BACKUP voltage supply and is ready for operation.
LAN IN		
ACT		The LED flashes briefly
LINK / ACT		The LEDs flash briefly just once
LINK		The LED blinks at regular intervals
LINK / ACT		The LED flashes briefly
ACT		The LED flashes
LINK / ACT		The LED flash at regular intervals
LINK / ACT		The LEDs are off
The traffic display is shown up on the LCD.		

5.5.3 STATUS DISPLAY PERFORMANCE UPON FIRMWARE UPDATE

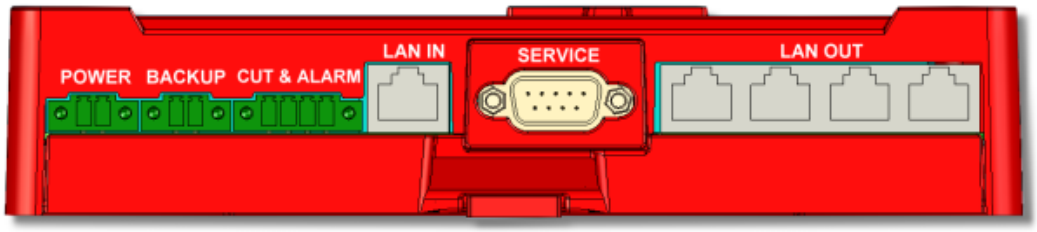
It is possible to execute firmware updates via the web interface. The actual update process may require a few mintues. During the update process, an indication thereof shows up on the LC display. The table herunder provides boot-up process LED blink frequency via which it is possible to check that the fiormware update process is being run correctly.



POWER	SIGNAL	ACTION
L+		The device is provided with voltage via POWER and is ready for operation.
BACKUP		
L+		The device is provided with BACKUP voltage supply and is ready for operation.
LAN IN		
LINK / ACT		The LEDs flash rapidly.
LINK / ACT		The LEDs flash briefly just once
		The LEDs are off
		The LEDs flash briefly just once
		The LEDs are off
LINK		The LED blinks at regular intervals
LINK / ACT		The LEDs flash briefly just once
		The LEDs are off
		The LEDs flash rapidly.
		The LEFT LED goes off / the ACT led goes on blinking
ACT		The LED flashes rapidly
		The LED is off
The traffic display is shown up on the LCD.		

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

5.6 INTERFACES



The device is provided with the following interfaces:

1. Power 24V DC voltage supply (2 pole COMBICON plug)
2. Backup 24V DC BACKUP voltage supply (2 pole COMBICON plug)
3. CUT& ALARM plug (4 pole COMBICON plug)
4. LAN-in with RJ45 (PoE) or LWL fibre optic connection
5. 9 pole SUB-D connector / RS232
6. LAN-out with 4x RJ45 connection

Note:
All input voltages can be hooked up redundantly (Power, Backup and PoE via LAN-in).

5.6.1 24V DC / BACKUP VOLTAGE SUPPLY

The supply voltage implements a lead-through terminal with screw connection (the illustration shows the jack provided in the device).

PIN-NUMBER	SIGNAL NAME
1	24V DC
2	0V DC

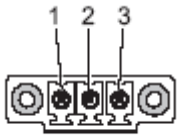


PIN 1: = L+ 24V DC voltage supply
PIN 2: = GND Ground

5.6.2 CUT & ALARM

The Cut & Alarm connection implements a lead-through terminal with screw connection (the illustration shows the connector provided in the device).

PIN-NUMBER	SIGNAL NAME
1	110/230 V AC
2	PE
3	0 V DC

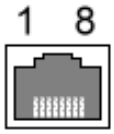


PIN 1: = L+ 24V DC feed-in of the alarm output voltage
PIN 2: = GND Ground feed-in of the alarm output voltage
PIN 3: = CUT 24V DC feed-in of an external switching signal (galvanically isolated)
PIN 4: = AL 24V DC ALARM output (galvanically isolated) alarm out put for signalling to external users

5.6.3 LAN-IN (RJ45) / POE (IEEE 802.AF) VOLTAGE SUPPLY

For voltage supply transmission the adapter-pair 4/5 is implemented for the plus pole whilst the lead-pair 7/8 is implemented for the minus pole.

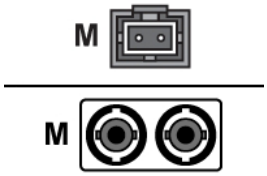
PIN-NUMBER	SIGNAL NAME
1	TX +
2	TX -
3	RX +
4	PoE/G
5	PoE/G
6	RX -
7	PoE/-48V
8	PoE/-48V



© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

5.6.4 LWL FIBRE OPTIC

An MTRJ fibre optic plug is implemented for the LWL fibre optic connection.62.5/125µm multimode cable from the MTRJ plug to the Duplex plug.

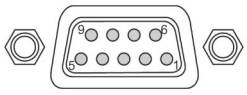


5.6.5 COM (RS232) SERIAL INTERFACE

9 pole SUB-D connector

RS232 for connection of an analogue, ISDN or GPRS standard modem unit.

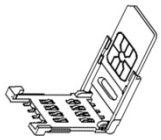
PIN-NUMMER	SIGNAL NAME
1	DCD
2	RxD
3	TxD
4	DTR
5	GND
6	DSR
7	RTS
8	CTS
9	RI

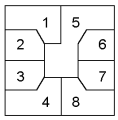


5.6.6 SIM CARD READER COMPLIANT TO ISO 7816

The SIM card reader serves for the storage of the configuration data.

PIN-NUMMER	SIGNAL NAME
1	VCC 5 Volt
2	RESET
3	CLOCK
4	n/c
5	GND
6	n/c
7	I/O
8	n/c





Note:

The interfaces as well as the device voltage/power supply plugs are arranged on the underside of the device. It is necessary to ensure that the plugs are protected against possible slip-outs.

6 Initial Device Operations

6.1 First-time Configuration



Warning:

First-time configuration of the device can only be executed via the LAN-in or LAN-out interfaces marked RJ45 / LWL fibre optic.

FIRST-TIME CONFIGURATION REQUIRES THAT THE DEVICE IS HOOKED UP TO A PC.

Hook-up of the 24V DC / PoE voltage supply source

The device can be powered with a **24V DC (2 pole plug)** voltage supply source or via a **PoE connection.** Furthermore, a **24V DC (2 pole plug)** is available for **backup connection** requirements. The corresponding COMBICON plug is supplied on issue with the device supply contents.

Connect up the device with teh appropriate voltage supply source.

Connection of the RJ45 / LWL fibre optic network cable

For first-time device operations a connection between the device and a PC via the RJ45/LWLfibre optic network cable is sitrictly required.

Connect the device up to a PC:

Device LAN-in / LAN-out connection <-> PC LAN connection

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

6.2 MANUAL CONFIGURATION OF THE NETWORK ADAPTER

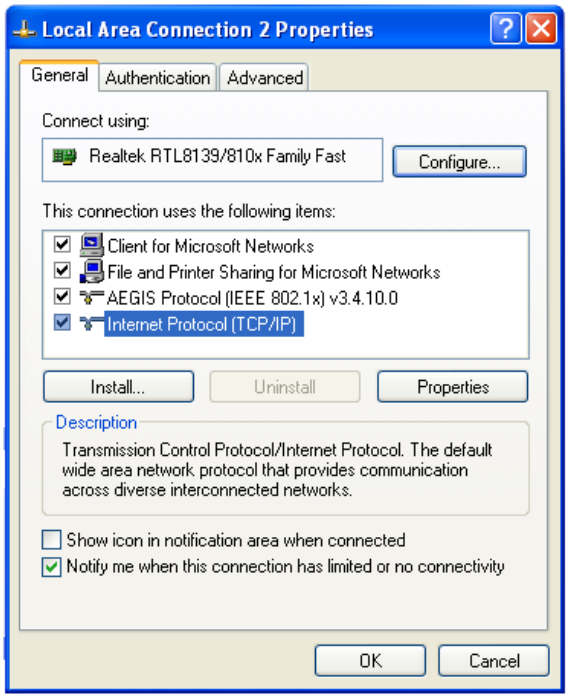
Note:

The procedural method described as follows was generated to serve as an example with the Microsoft Windows XP professional® operating system. If another operating system was implemented instead, the paths and properties described herein may vary.

Now access you network adapter properties map. The relative path is as follows:

Network connections> LAN connection> Properties (righ-click on your mouse).

In the dialogue tab that come sup on screen, click to select option: **Internet protocol (TCP/IP)** then click on the **Properties** selection box.



Simply click to select: **Use the following IP address**

Acces to the device is only enabled when the following parameters are recorded as the fixed IP address or if the computer is located in the same subnet space:

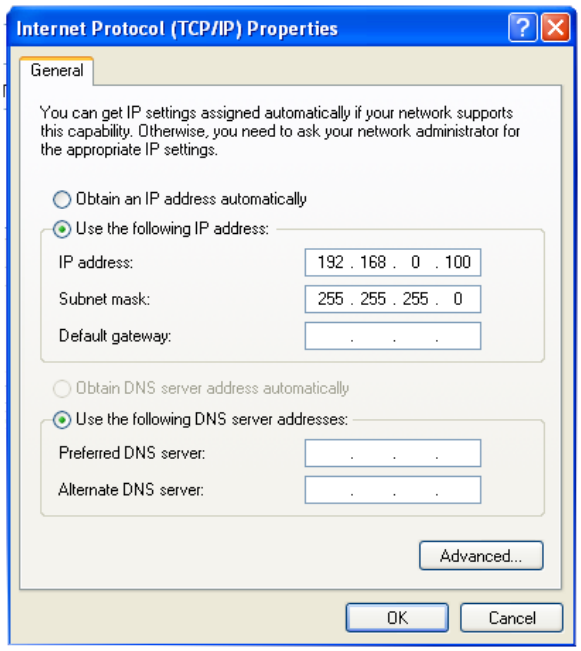
IP ADDRESS: 192.168.0.100

Note:

*The last set of digits must be a number between 1 and 253. In the example, "**100**" has been selected.*

Once the IP address has been recorded, the subnet mask address must be recorded. Click directly on the Subnet mask field will and the correct address will pop in.

SUBNET MASK: 255.255.255.0


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 0 . 100
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

It is now possible to close and exit the dialogue tab by clicking on the "**OK**" button.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

6.3 SETTINGS FOR USE WITH INTERNET EXPLORER 8

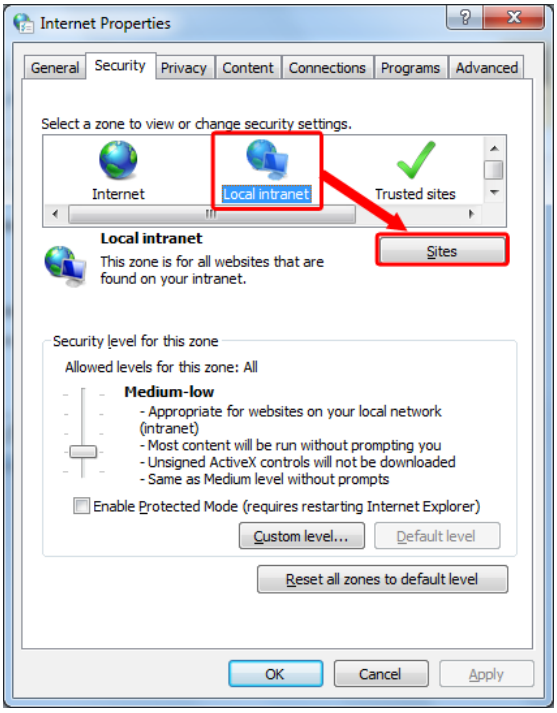
Warning:

If Internet Explorer 8 is used, issues with the web interface might occur. If you experience any problems, the IP address of the device must be entered in the Local Intranet list in order to display the web interface correctly.

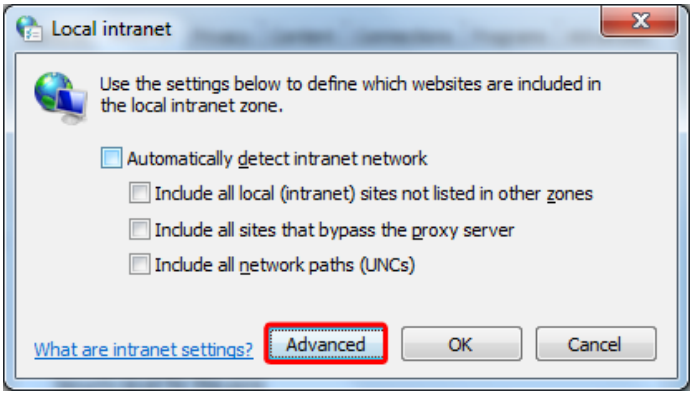
Open Internet Explorer and navigate to the **Security** tab with the following directory path:

Tools→Internet options→Security

Switch to the **Local Intranet** tab and click there on **Sites**.



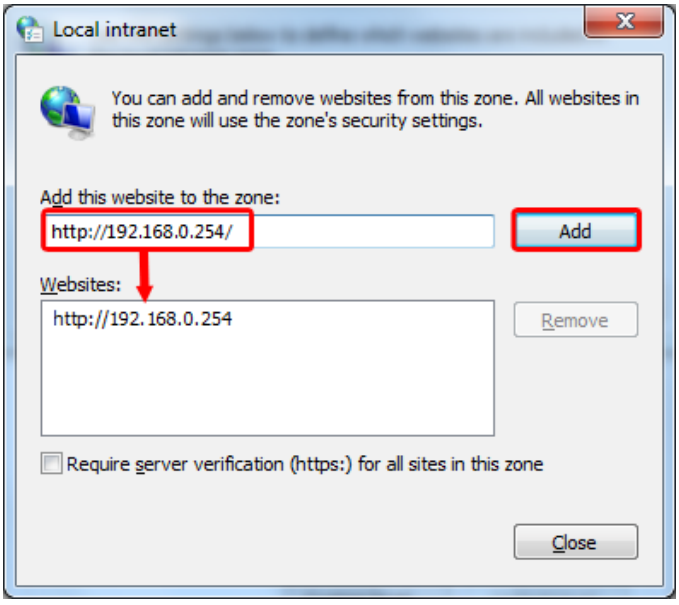
Then click on **Advanced**.


Local intranet
Use the settings below to define which websites are included in the local intranet zone.
Automatically detect intranet network
Include all local (intranet) sites not listed in other zones
Include all sites that bypass the proxy server
Include all network paths (UNCs)
What are intranet settings?
Advanced
OK
Cancel

In the **Add this website to the zone** address line, enter the device **IP address** and confirm this step with **Add**.

Default IP address: **http://192.168.0.254**

The entered **IP address** should now appear in the list under **Websites**.


Local intranet
You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.
Add this website to the zone:
http://192.168.0.254/
Add
Websites:
http://192.168.0.254
Remove
Require server verification (https:) for all sites in this zone
Close

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

6.4 CALLING UP THE DEVICE WEB INTERFACE

To access and open the device web interface, start up your web browser. In the browser's address bar, enter the following IP address then confirm with **Enter**

http://192.168.0.254

LOGIN

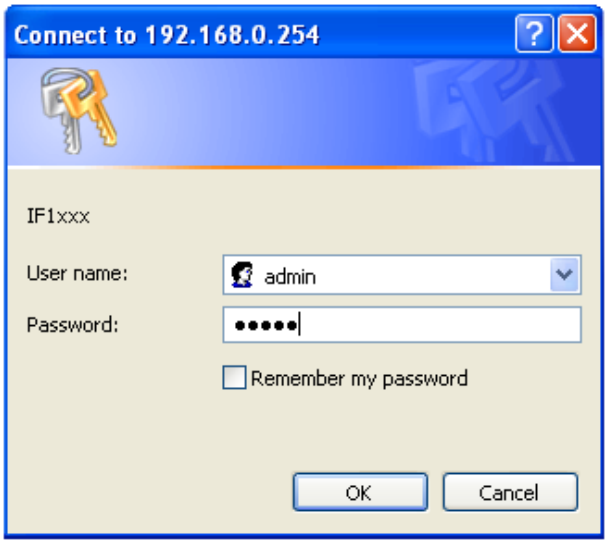
Once the IP address has been entered with success, the login prompt appears. In the login prompt, entry of the default settings is required.

The default configuration in just-delivered conditions is:

USER NAME **:** **admin**

PASSWORD : **admin**

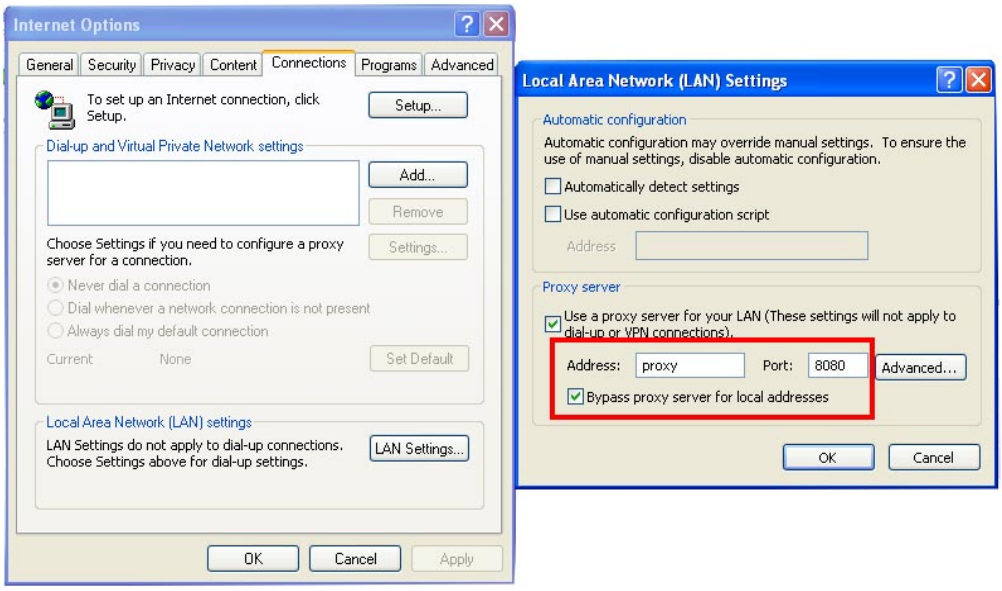
Confirm your entries by clicking on: **OK**



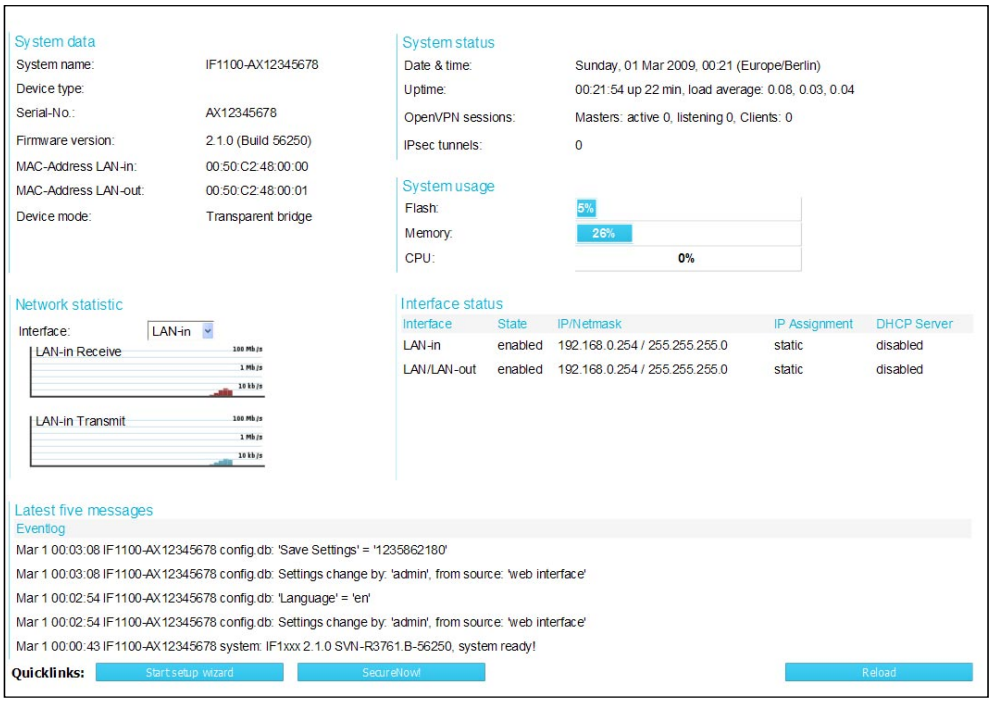
Note:

If the login prompt does not appear, check to ensure that the device has been connected via a RJ45/LWL optic fibre connection cable. Otherwise, connect the device up to a PC (Device LAN-in/LAN-out connection <> PC LAN connection).

If there still is no connection to the firewall login prompt, it is necessary to check the proxy and local firewall settings. It often occurs that also local subnet addresses (e.g. 192.168.x.x) are diverted to a proxy server. In this case it is possible to select the "Bypass proxy server for local addresses" option to enter the address in question.



Finally, the device web interface will come up on screen.


System data
System name: IF1100-AX12345678
Device type:
Serial-No.: AX12345678
Firmware version: 2.1.0 (Build 56250)
MAC-Address LAN-in: 00:50:C2:48:00:00
MAC-Address LAN-out: 00:50:C2:48:00:01
Device mode: Transparent bridge
System status
Date & time: Sunday, 01 Mar 2009, 00:21 (Europe/Berlin)
Uptime: 00:21:54 up 22 min, load average: 0.08, 0.03, 0.04
OpenVPN sessions: Masters: active 0, listening 0, Clients: 0
IPsec tunnels: 0
System usage
Flash: 5%
Memory: 26%
CPU: 0%
Network statistic
Interface: LAN-in
LAN-in Receive
LAN-in Transmit
Interface status
Interface State IP/Netmask IP Assignment DHCP Server
LAN-in enabled 192.168.0.254 / 255.255.255.0 static disabled
LAN/LAN-out enabled 192.168.0.254 / 255.255.255.0 static disabled
Latest five messages
Eventlog
Mar 1 00:03:08 IF1100-AX12345678 config.db: 'Save Settings' = '1235862180'
Mar 1 00:03:08 IF1100-AX12345678 config.db: Settings change by: 'admin', from source: 'web interface'
Mar 1 00:02:54 IF1100-AX12345678 config.db: 'Language' = 'en'
Mar 1 00:02:54 IF1100-AX12345678 config.db: Settings change by: 'admin', from source: 'web interface'
Mar 1 00:00:43 IF1100-AX12345678 system: IF1xxx 2.1.0 SVN-R3761.B-56250, system ready!
Quicklinks:
Start setup wizard
SecureNow!
Reload

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

7 Firewall Setup Assistant

For a quick and easy start-up and configuration of the firewall, two setup assistants are integrated. With the aid of the setup assistants a guided configuration process of the language settings, the operation modes as well as the password is provided. Via the filter assistants, a guided configuration process of the filter rules is provided. Further information is provided in the Filter Assistant section herein. All settings can also be changed through the web interface, independently of the assistants.

7.1 First-time Configuration with the help of the setup assistants

To carry out a basic configuration, in the **Quicklinks** field on the start page, select:

Start Setup Assistant

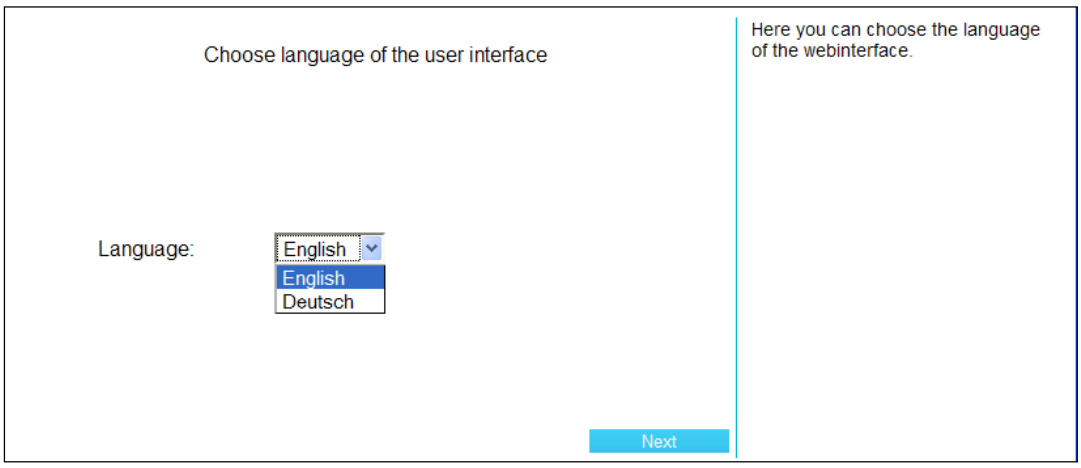
Note:

The question mark to the right near the drop-down menu provides directions and brief explanations concerning the menu points available for selection.

Said directions and brief explanations are correctly provided with Microsoft© Internet Explorer as of Version 7 and Mozilla Firefox© as of Version 1.0.

Language Selection

Via the dialogue window it is possible to set the user interface language.

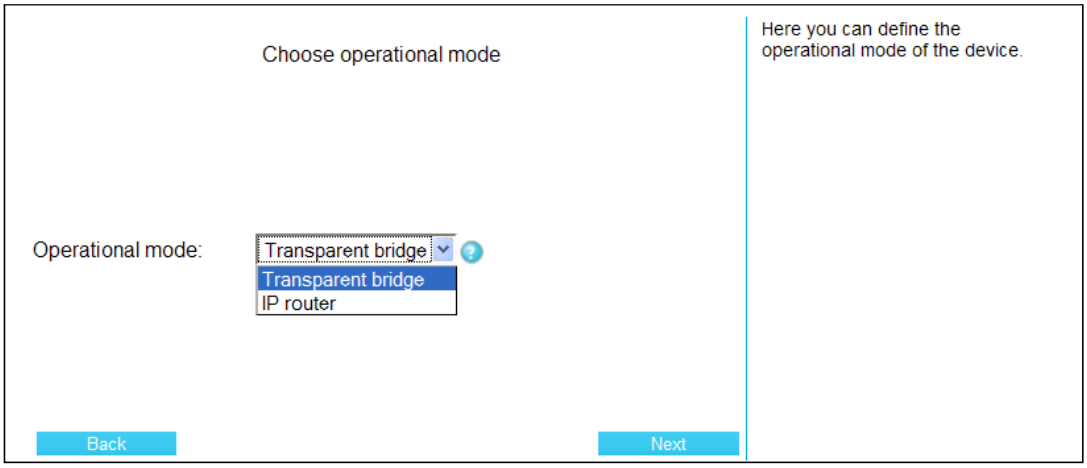


The selected language is used for the overall web interface and the LC display.

Confirm your entries by clicking on: **Next**

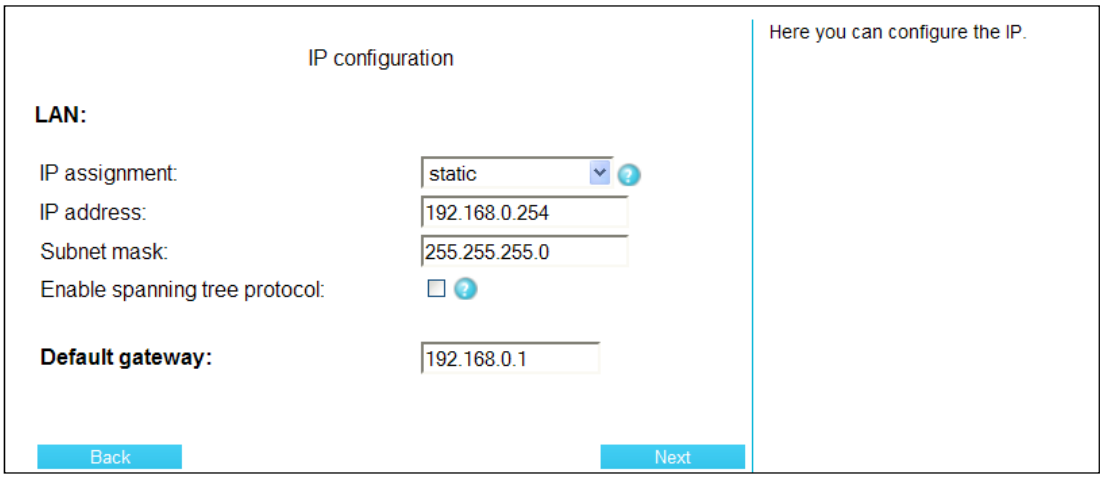
OPERATION MODE SELECTION

The operation mode can be selected between **Transparent Bridge** and **IP Router**.

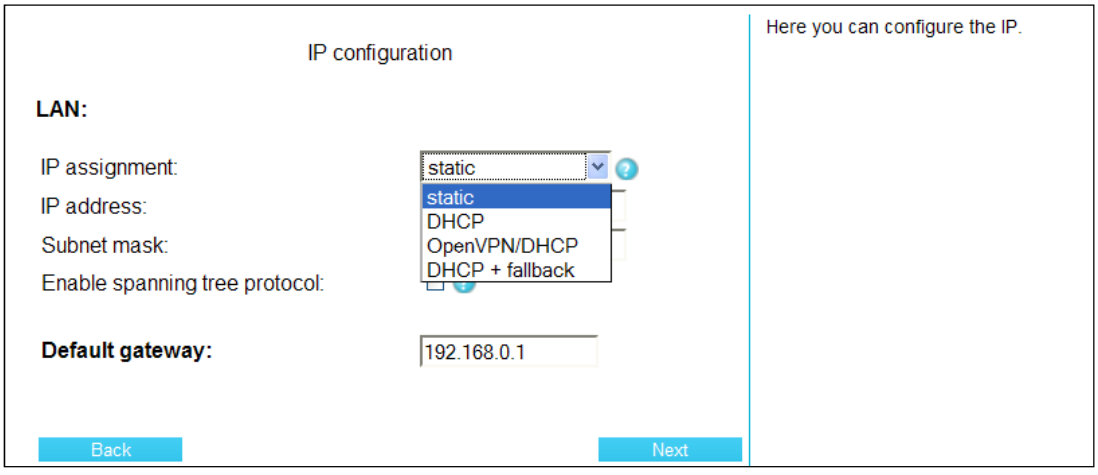


7.1.1 TRANSPARENT BRIDGE

In the transparent bridge mode, the firewall acts as a Layer 2 bridge and is invisible to participants.



The following options are available for IP assignment:



© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

Static:

If this option is selected, it is possible to record a fix-allocated IP address. Static IP assignment requires entry of the IP address and subnet mask.

The default values are:

IP address: **192.168.0.254**

Subnet mask: **255.255.255.0**

DHCP:

The DHCP function requests an Ip address from a DHCP server and proceeds with allocation automatically.

OpenVPN/DHCP:

The IP address assignment is configured by an OpenVPN connection.



Note:

This setting requires additional input in menu OpenVPN.

DHCP fallback:

This option allows for automatic allocation of the IP address. Should there be an error with the automatic allocation, the IP assignment automatically switches to the static setting option. For this reason, selection of DHCP fallback always requires the entry of an IP address and subnet mask.



Note:

Access to the device is only enabled when the computer is located in the same subnet space as the Firewall.

Activate Spanning Tree Protokoll:

The Spanning Tree Protocol (STP) constitutes a tree structure for the prevention of redundant network paths (loops) in the LAN, especially in switched environments. Implementation essentially underlies a Spanning Tree Algorithm (to the IEEE Standard 802.1D).

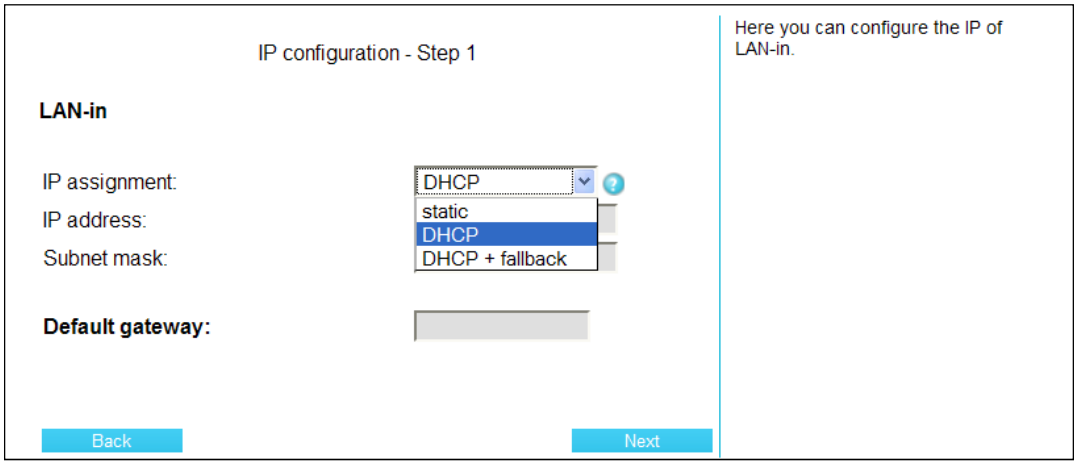
The Spanning Tree Protokoll also serves for the build-up of redundant network paths, especially in switched environments.

Confirm your selection by clicking on: **Next.**

7.1.2 IP Router

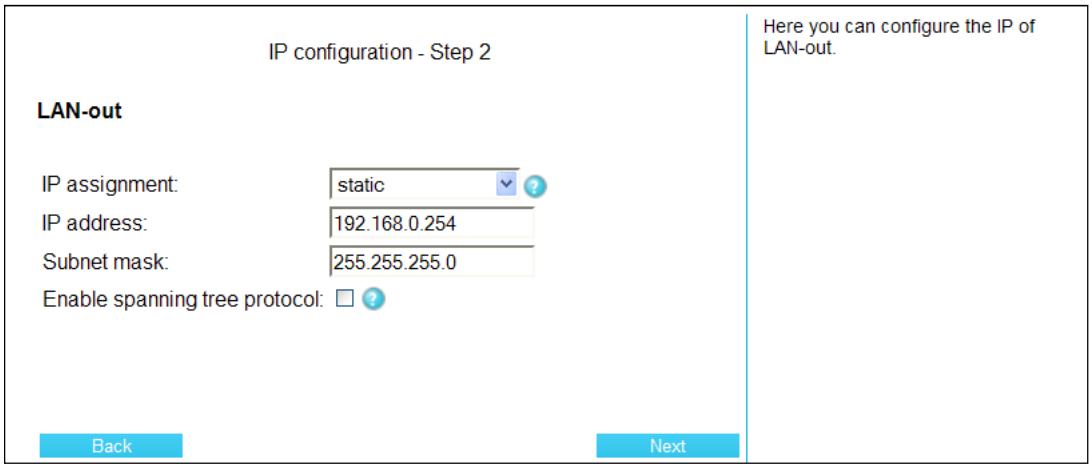
The firewall divides the nets between the LAN-in and LAN-out interfaces into two separate nets and filters them separately. It is for this reason that in this operating mode two independent addresses for LAN-in and LAN-out need to be allocated.

In the IP-Router operation mode the LAN-in and LAN-out interfaces are configured consecutively.



Select the LAN-in interface for the IP assignment to be used and enter all the required data.

Confirm by clicking on: **Next**



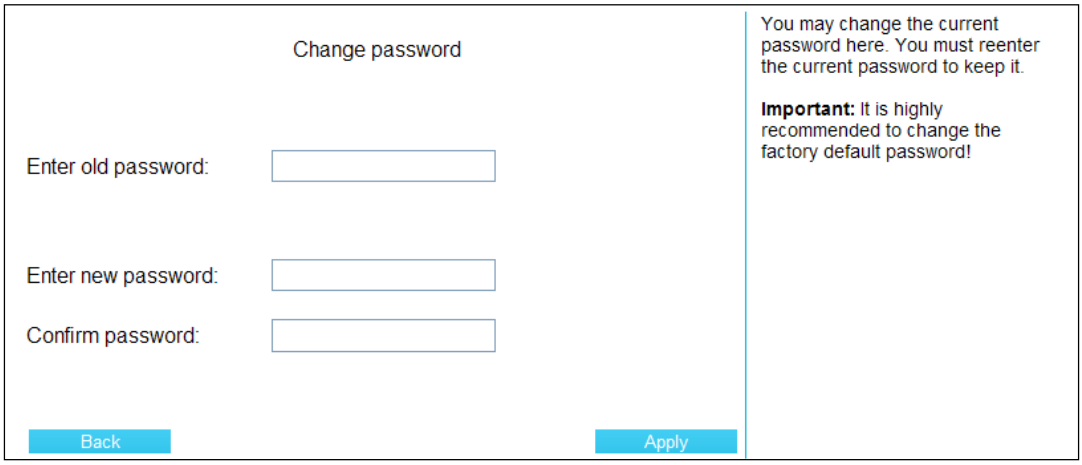
Select the LAN-out interface for the IP assignment to be used and enter all the required data. The Spanning Tree Protocol can also furthermore be activated.

Confirm by clicking on: **Next**

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

7.1.3 PASSWORD CHANGE

Via the dialogue window, it is possible to change the Password.


Change password
Enter old password:
Enter new password:
Confirm password:
Back
Apply
You may change the current password here. You must reenter the current password to keep it.
Important: It is highly recommended to change the factory default password!

To change an already allocated password, enter the current password into the **Old password** field.

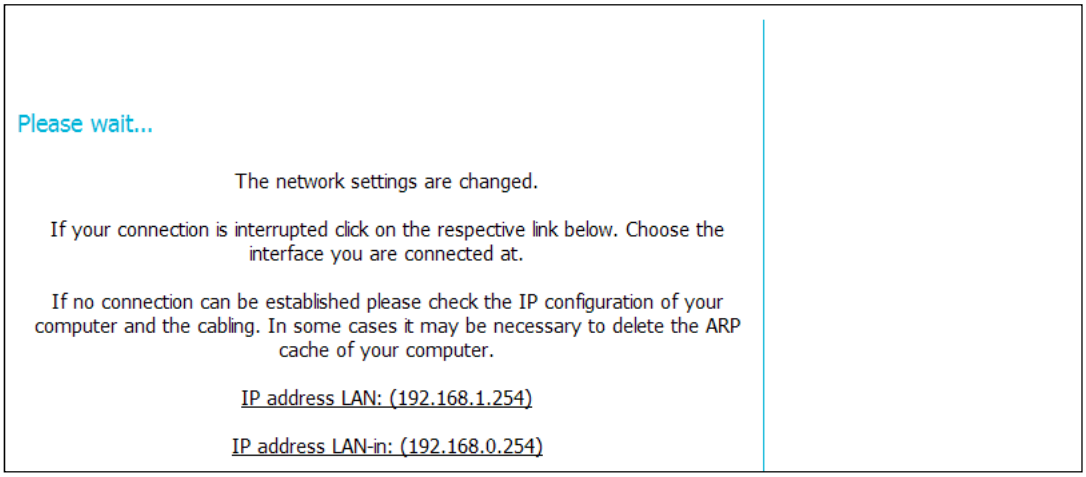
Enter another password in the **New password** field, then reconfirm it by entering it again into the **Password confirmation** field.

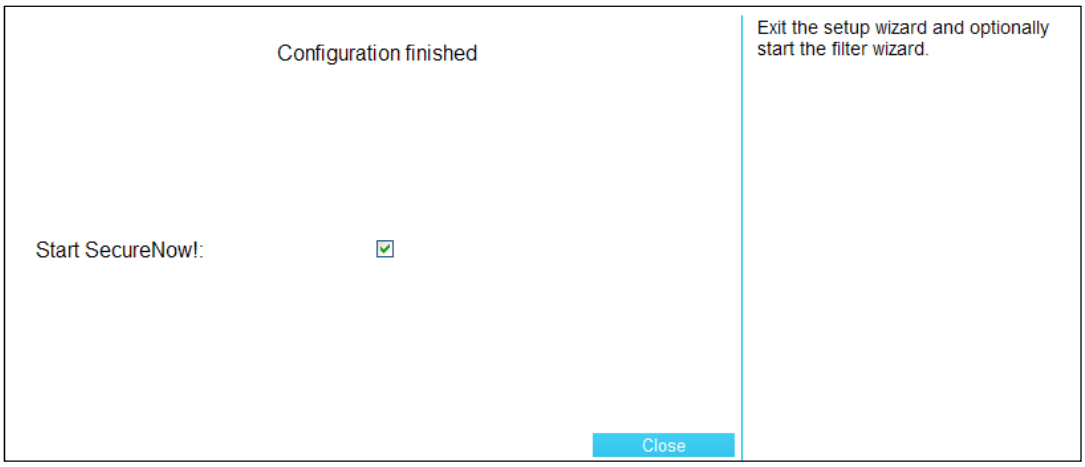
If you no longer wish to change the password, leave the fields free.

Finally, click on: **Apply**

7.1.4 SETTING ACTIVATION

Your settings are now activated.


Please wait...
The network settings are changed.
If your connection is interrupted click on the respective link below. Choose the interface you are connected at.
If no connection can be established please check the IP configuration of your computer and the cabling. In some cases it may be necessary to delete the ARP cache of your computer.
IP address LAN: (192.168.1.254)
IP address LAN-in: (192.168.0.254)



Note:

*Should you not wish to begin directly upon connection with the filter configuration, remove the check marks at "**Start SecureNow!**".*

Subsequent to the setup assistents comes SecureNow!. Close configuration by clicking on **Close**.

The setup assistent is thus closed.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

7.2 SECURENOW!

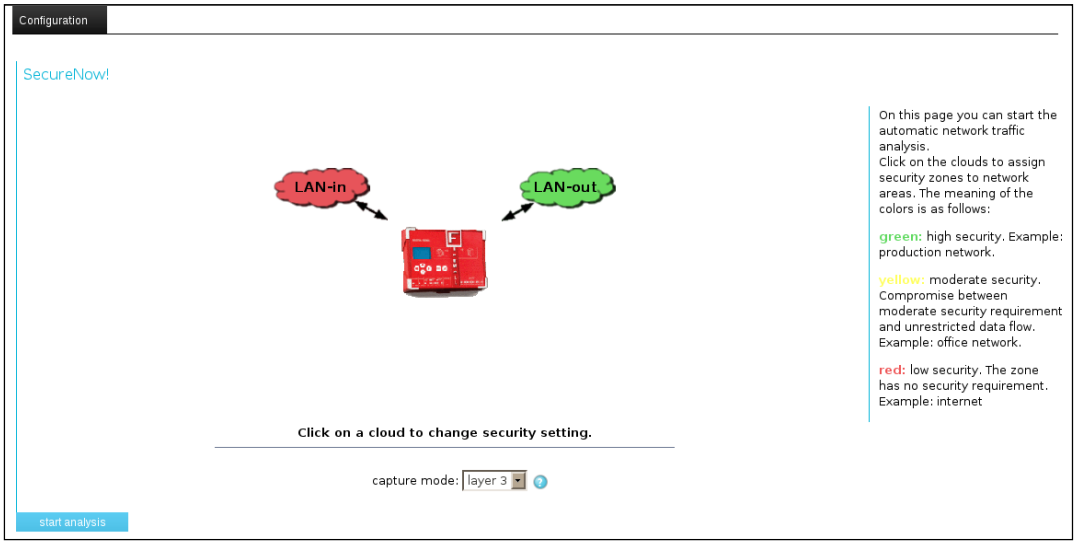
GENERAL INFO

SecureNow! allows everybody the achievement of a maximum security for local networks with only very little interaction. In order to ensure this, SecureNow! is analysing the network traffic passing through the industrial firewall and is generating precisely tailored filer rules for ebtables (in Transbridge mode) or iptables (in IPRouter or IPRouter5Port mode) based on this information.

START PAGE

At the start, the user defines for all enabled interfaces of the IF1000 series device individually, which security requirements apply. Three security levels are available for selection: High, medium and low. SecureNow! is going to generate particularly strict rules for a zone with high security level. With the medium security level, the rules are less strict in order to meet requirements like they would be present in office networks, for instance. The low security level should be used for the uplink, e.g. for the interface connected with the Internet. This zone's rules are strict with respect to the traffic coming from it, on one hand. But the traffic directed from the higher security level to the lower one is - if in doubt - always permitted. This, as a result, is always valid for the lowest level.

The network traffic recognised as critical for security is an exception. In order to recognise it, SecureNow! has a database, in which frequently used protocols are evaluated with respect to their security.


Configuration
SecureNow!
LAN-in
LAN-out
On this page you can start the automatic network traffic analysis.
Click on the clouds to assign security zones to network areas. The meaning of the colors is as follows:
green: high security. Example: production network.
yellow: moderate security. Compromise between moderate security requirement and unrestricted data flow. Example: office network.
red: low security. The zone has no security requirement. Example: internet
Click on a cloud to change security setting.
capture mode: layer 3
start analysis

The user can switch to the next security level by simply clicking with the mouse on one of the clouds. On the right hand side, you'll find a note explaining the significance of the zones by means of examples.

Note:

If two networks are identified with the same colour (e.g. yellow), the rules for the traffic between these zones will allow all packets.

Note:

Additional information for "SecureNow!" can be seen in the sections of the web interface and the relevant Use-Cases.

7.3 CONFIGURATION WITH THE HELP OF THE PACKET FILTER

A packet filter located in the firewall is reponsible for the classification of both desired and non-desired data traffic and for the initiation of the corresponding actions.

If not started directly subsequent to the start of the **Start Assistants** over SecureNow!**,** the packet filter can be started via the **Configuration > Packet filter** path.

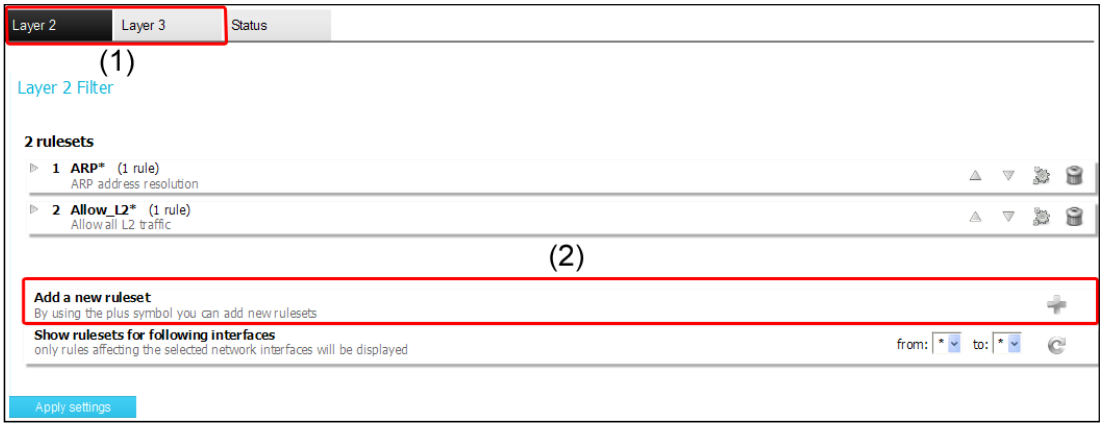
The Packet filter start page allow for the addition of new rule sets as well as the processing and cancellation of existing rule sets.

Note:

A rule describes the configuration of a specific filter command. A rule set can consist of up to 10 separate rules.

7.3.1 ADDITION OF A RULE SET

The addition of a rule set requires first of all the selection of the layer via the particular **tab (1)**. In transparent bridge mode, in most cases a filtering on layer 2 is required, whilst in IP router mode or if using the SERVICE modem, selection of layer 3 may also come into question.



Bridged Ethernet interfaces (Layer 2):

is equivalent to the Ethernet filtering layer. This setting allows e.g. for the filtering based on the Ethernet MAC addresses or network protocols that do not employ IP addresses. Nevertheless, a filter on the basis of IP protocol criteria is also possible.

Standalone IP-Interfaces (Layer 3):

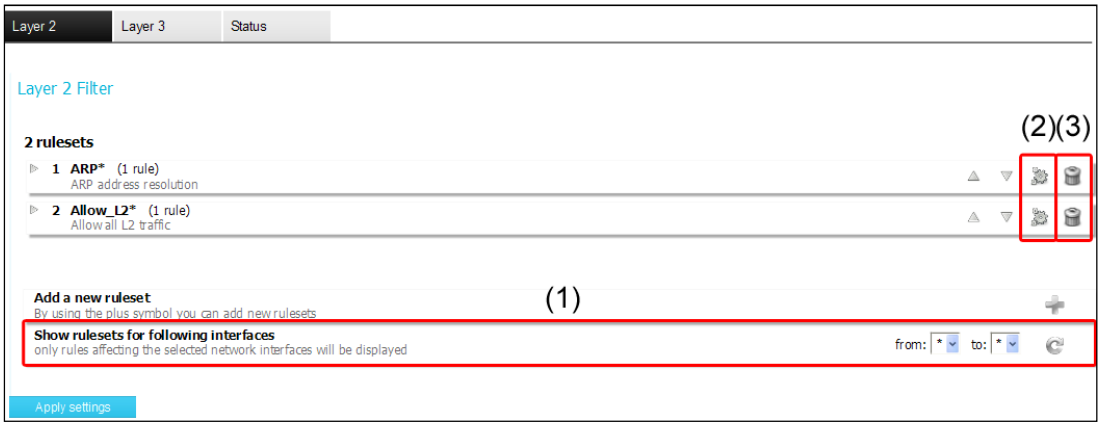
On this layer, filtering is possible exclusively on the basis of IP protocol criteria in that between layer 3 interfaces, it is exclusively IP data traffic that takes place.

Via the Adding (2) button, it is possible to generate or to add on a new or pre-configured rule to the selected layer. You will find a description on the generation of a new rule set under the **Defintion of a new rule set on layer 2** and **Definition of a new rule set on layer 3** sections herein. In the **Pre-configured rule set upload** section, a description of the pre-defined rule sets is provided.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

7.3.2 CHANGING AND SEARCHING EXISTING RULE SETS

If rules have already been generated or uploaded, they appear in the relative rule summary. If searching for a rule, the filter criteria for the rule set being sought can be restricted via the drop-down fields **From** and **To** (**1**).



The **Edit** (**2**) button allows for the subsequent variation of the selected rule sets. By way of the **Delete** (**3**) option, it is possible to remove the selected rule set.

Note:

By using the arrows in front of the ruleset, detailled information to the selected ruleset is will be shown.

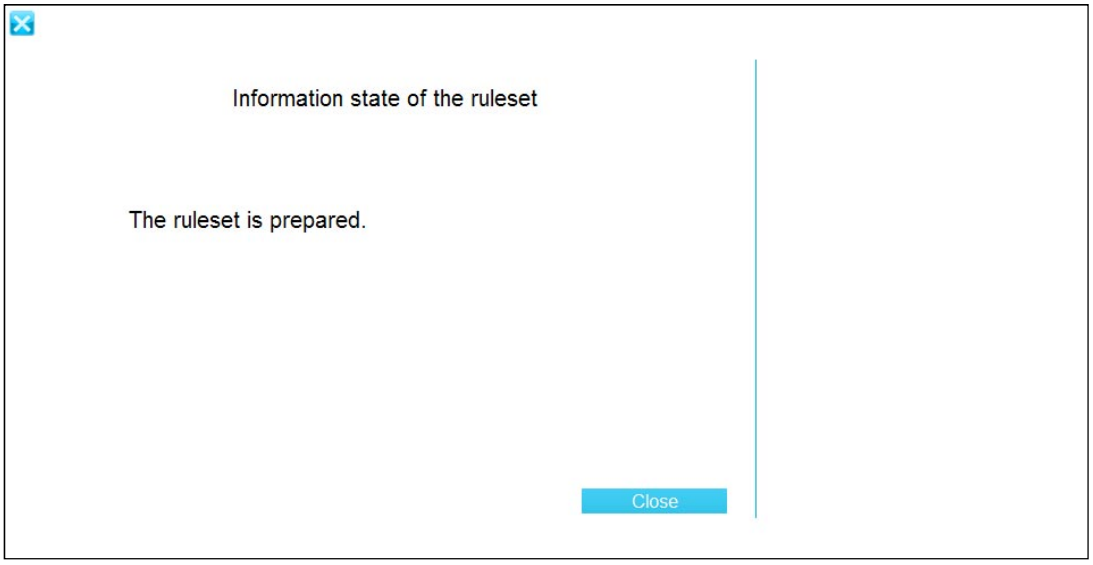
7.3.3 PRE-CONFIGURED RULE-SET UPLOAD

Select a pre-configured rule set.

The dialogue window show the pre-configured rule sets to the left.


Choose an existing ruleset or create a new one
Rulesets for layer 2
PTP_FRLO
RTPS_FRLI
RTPS_FRLO
SMTP_FRLI
SMTP_FRLO
TELNT_FRLI
TELNT_FRLO
WIN_FRLI
WIN_FRLO
Define a new ruleset
Name of the ruleset:
RTPS_FRLI
Description of the ruleset:
Allow Realtime Publish Subscribe Protocol from a client connected to LAN-in
Here you can select an existing ruleset or create a new one.
Further on, you can delete existing self defined rulesets.
Predefined rulesets can be modified after copying a selected ruleset with the copy button.
A ruleset may have up to 10 filter rules. Currently active rulesets are greyed out and cannot be selected.
Delete
Copy
Close
Next

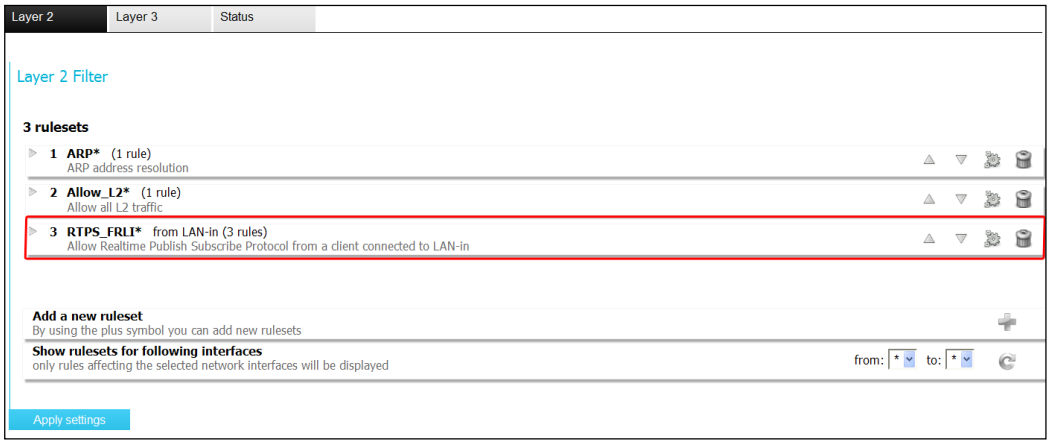
Select the required pre-configured rule set, and confirm by clicking on: Next



Confirm your entries as shown on display by clicking on: **Close**

Successful selection will show the rule set in the filter overview. To activate the modified rule set list click on **Activate.**

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen


Layer 2
Layer 3
Status
Layer 2 Filter
3 rulesets
1 ARP* (1 rule)
ARP address resolution
2 Allow_L2* (1 rule)
Allow all L2 traffic
3 RTPS_FRLI* from LAN-in (3 rules)
Allow Realtime Publish Subscribe Protocol from a client connected to LAN-in
Add a new ruleset
By using the plus symbol you can add new rulesets
Show rulesets for following interfaces
only rules affecting the selected network interfaces will be displayed
from: * to: *
Apply settings

By way of example, the following standard rule sets are already pre-configured in layer levels 2 and 3.

RULE SETS FOR BRIDGED ETHERNET INTERFACES (LAYER 2):

Name	Brief description
ARP	Address Resolution Protocol allows for the assigment of network addresses to hardware addresses.
Alarm_L2	Sets off the alarm signal, logs the event in the event log and overrules all the data packets.
Allow_L2	Enables overall data traffic on layer 2.
Block_L2	Overrules all the data packets (blocks the overall data traffic) on layer 2.
Cut_L2	Sets off the internal Cut, logs the event in the event log and overrules all the data packets on layer 2.
E_CAT_FRLI	Allows for the EtherCAT protocol related data traffic through LAN-in to LAN-out.
E_CAT_FRLO	Allows for the EtherCAT protocol related data traffic through LAN-out to LAN-in.
E_NET_FRLI	Allows for the EtherNET/IP protocol-related data traffic through LAN-in to LAN-out.
E_NET_FRLO	Allows for the EtherNET/IP protocol-related data traffic through LAN-out to LAN-in.
HTTPS_FRLI	Allows for the HTTPS related data traffic through LAN-in to LAN-out.
HTTPS_FRLO	Allows for data traffic through HTTPS through LAN-out to LAN-in.
HTTP_FRLI	Allows for data traffic through HTTPS through LAN-in to LAN-out.
HTTP_FRLO	Allows for data traffic through HTTPS through LAN-out to LAN-in.
ICMP_L2	Enables overall data traffic through ICMP on layer 2.
IMAP_FRLI	Allows for data traffic via IMAP TCP through LAN-in to LAN-out.
IMAP_FRLO	Allows for data traffic via IMAP TCP through LAN-out to LAN-in.
Log_L2	Logs events in the event log and overrules all the data packets on layer 2.
MODBS_FRLI	Allows for data traffic via MODBUS TCP through LAN-in to LAN-out.
MODBS_FRLO	Allows for data traffic via MODBUS TCP through LAN-OUT to LAN-in.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

NC@P_FRLI	Allows for data traffic of all the NETC@P packets through LAN-in to LAN-out.
NC@P_FRLO	Allows for data traffic of all the NETC@P packets through LAN-out to LAN-in.
POP_FRLI	Allows for all POP TCP connections through LAN-in to LAN-out.
POP_FRLO	Allows for all POP TCP connections through LAN-out to LAN-in.
PRNET_FRLI	Allows for data traffic of all the PROFINET packets through LAN-in to LAN-out.
PRNET_FRLO	Allows for data traffic of all the PROFINET packets through LAN-out to LAN-in.
PTP_FRLI	Allows for Precision protocol-related data traffic through LAN-in to LAN-out.
PTP_FRLO	Allows for Precision protocol-related data traffic through LAN-out to LAN-in.
RTPS_FRLI	Allows for Realtime Publish Subscribe protocol-related data traffic through LAN-in to LAN-out.
RTPS_FRLO	Allows for Realtime Publish Subscribe protocol-related data traffic through LAN-out to LAN-in.
SMTP_FRLI	Allows for data traffic of all the SMTP TCP packets through LAN-in to LAN-out.
SMTP_FRLO	Allows for data traffic of all the SMTP TCP packets through LAN-out to LAN-in.
TELNT_FRLI	Allows for data traffic of all the TELNET packets through LAN-in to LAN-out.
TELNT_FRLO	Allows for data traffic of all the TELNET packets through LAN-out to LAN-in.
WIN_FRLI	Allows for data traffic of all the Microsoft Windows Networking packets through LAN-in to LAN-out.
WIN_FRLO	Allows for data traffic of all the Microsoft Windows Networking packets through LAN-out to LAN-in.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

RULE SETS FOR STANDALONE IP-INTERFACES LAYER 3

Name	Brief description
Alarm_L3	Sets off the alarm signal, logs the event in the event log and overrules all the data packets.
ALLOW_L3	Enables overall data traffic on layer 2.
BLOCK_L3	Blocks overall data traffic on layer 2.
Cut_L3	Sets off the internal Cut, logs the event in the event log and overrules all the data packets.
E_CAT_FRLI	Allows for the EtherCAT protocol related data traffic through LAN-in to LAN-out.
E_CAT_FRLO	Allows for the EtherCAT protocol related data traffic through LAN-out to LAN-in.
E_NET_FRLI	Allows for the EtherNET/IP protocol-related data traffic through LAN-in to LAN-out.
E_NET_FRLO	Allows for the EtherNET/IP protocol-related data traffic through LAN-out to LAN-in.
FTP_FRLI	Allows for the FTP data traffic through LAN-in to LAN-out.
FTP_FRLO	Allows for the FTP data traffic through LAN-out to LAN-in.
HTTPS_FRLI	Allows for the HTTPS related data traffic through LAN-in to LAN-out.
HTTPS_FRLO	Allows for data traffic through HTTPS through LAN-out to LAN-in.
HTTP_FRLI	Allows for data traffic through HTTPS through LAN-in to LAN-out.
HTTP_FRLO	Allows for data traffic through HTTPS through LAN-out to LAN-in.
ICMP_L3	Enables overall data traffic through ICMP on layer 3.
IMAP_FRLI	Allows for data traffic via IMAP TCP through LAN-in to LAN-out.
IMAP_FRLO	Allows for data traffic via IMAP TCP through LAN-out to LAN-in.
Log_L3	Logs events in the event log and overrules all the data packets on layer 3.
MODBS_FRLI	Allows for data traffic via MODBUS TCP through LAN-in to LAN-out.
MODBS_FRLO	Allows for data traffic via MODBUS TCP through LAN-OUT to LAN-in.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

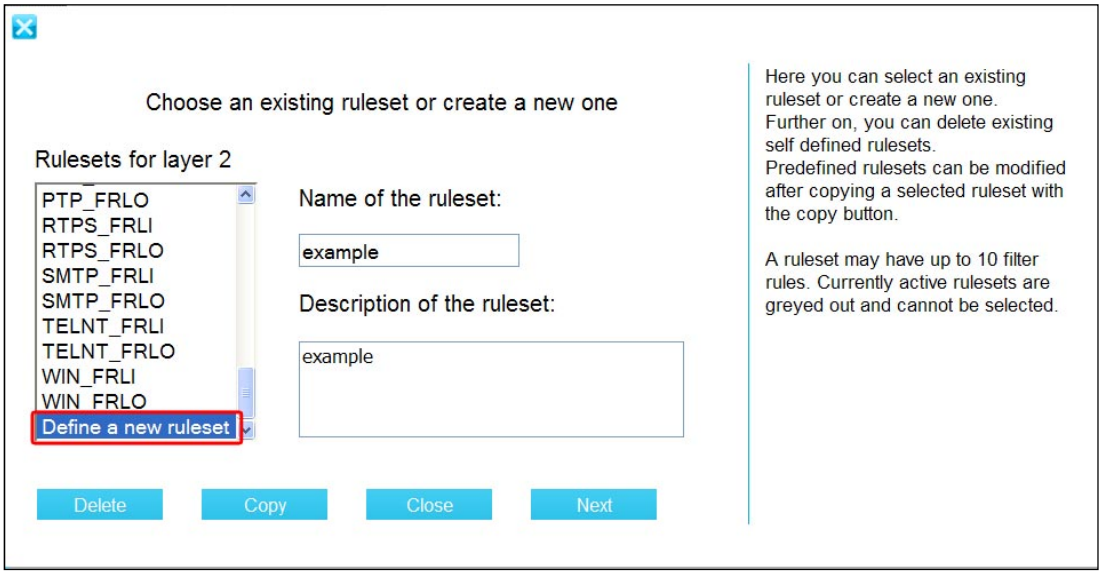
NC@P_FRLI	Allows for data traffic of all the NETC@P packets through LAN-in to LAN-out.
NC@P_FRLO	Allows for data traffic of all the NETC@P packets through LAN-out to LAN-in.
POP_FRLI	Allows for all POP TCP connections through LAN-in to LAN-out.
POP_FRLO	Allows for all POP TCP connections through LAN-out to LAN-in.
PRNET_FRLI	Allows for data traffic of all the PROFINET packets through LAN-in to LAN-out.
PRNET_PRLO	Allows for data traffic of all the PROFINET packets through LAN-out to LAN-in.
PTP_FRLI	Allows for Precision protocol-related data traffic through LAN-in to LAN-out.
PTP_FRLO	Allows for Precision protocol-related data traffic through LAN-out to LAN-in.
RTPS_FRLI	Allows for Realtime Publish Subscribe protocol-related data traffic through LAN-in to LAN-out.
RTPS_FRLO	Allows for Realtime Publish Subscribe protocol-related data traffic through LAN-out to LAN-in.
SMTP_FRLI	Allows for data traffic of all the SMTP TCP packets through LAN-in to LAN-out.
SMTP_FRLO	Allows for data traffic of all the SMTP TCP packets through LAN-out to LAN-in.
TELNT_FRLI	Allows for data traffic of all the TELNET packets through LAN-in to LAN-out.
TELNT_FRLO	Allows for data traffic of all the TELNET packets through LAN-out to LAN-in.
WIN_FRLI	Allows for data traffic of all the Microsoft Windows Networking packets through LAN-in to LAN-out.
WIN_FRLO	Allows for data traffic of all the Microsoft Windows Networking packets through LAN-out to LAN-in.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

7.3.4 DEFINITION OF A NEW RULE SET ON BRIDGED ETHERNET INTERFACES (LAYER 2)

Note:
*Should you need to configure layer 3 filter levels, please go on to the **Definition of a new rule set on layer 3** section herein.*

Select menu item: **Define a new rule set**



Enter a name and a description for the new rule set.

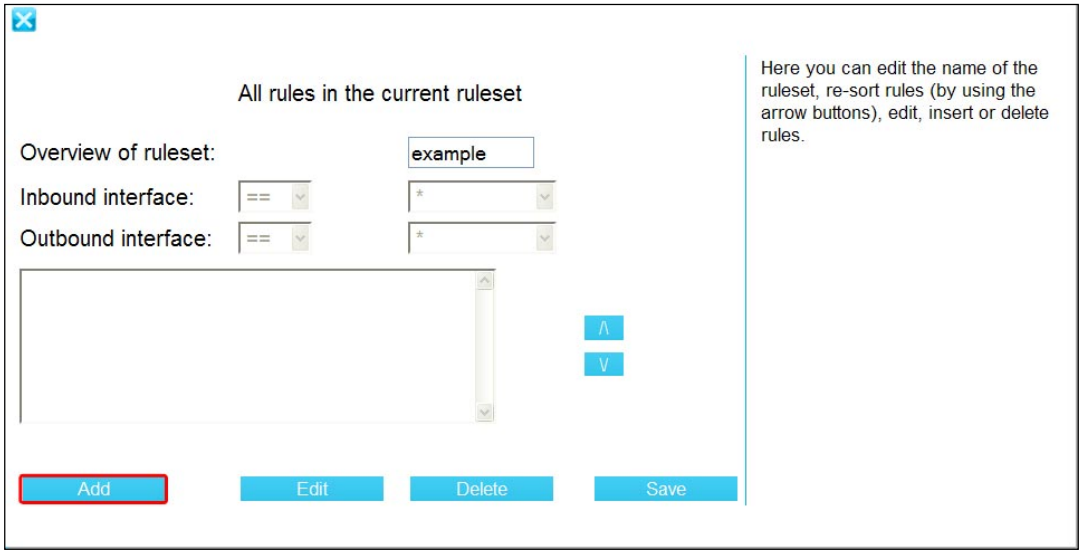
Note:
The rule set name is restricted to 16 characters. It is not possible to use umlauts.

Confirm your entries by clicking on **Next**.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

ALL RULES IN THE CURRENT RULESET

Via the dialogue window the path of the packets on which the rule set is to be implemented, is set up. An inbound interface (via which the packets are entered) as well as an outbound interface (via which the device packets are released subsequent to acceptance) are required.



Symbol description	
==	The selected interface is implemented.
!=	All interfaces are implemented, **except for** the selected interface

EXAMPLE:

Interface	Selection	Result
Inbound interface: **LAN-in**	==	filters all the inbound data packets on LAN-in
Outbound interface **LAN-out**	!=	filters all the outbound data packets on all ports, **except for LAN-out**

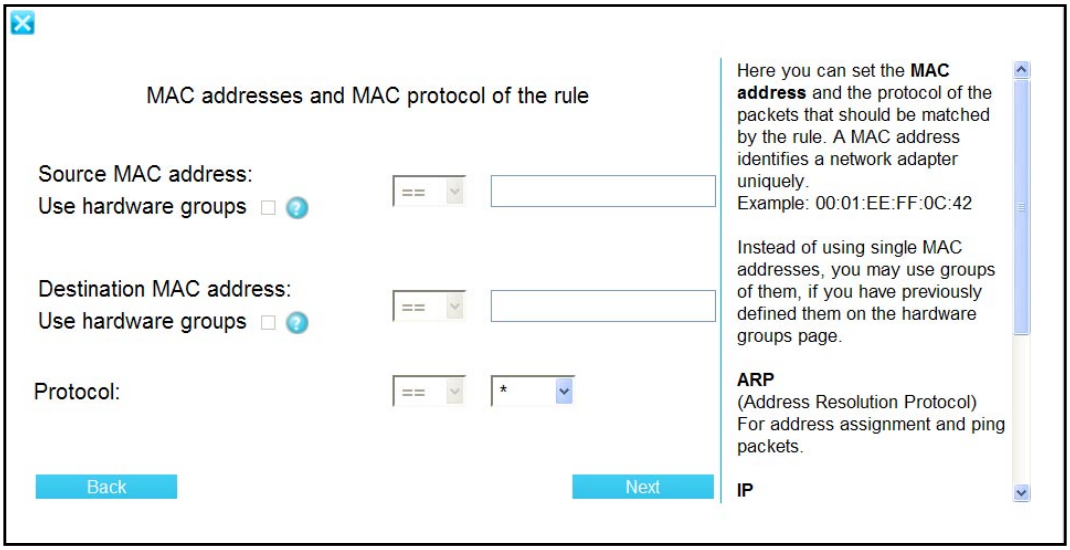
Confirm your entries by clicking on: **Next**

MAC ADRESSES AND MAC PROTOCOLS RELATED TO THE RULES

Via the dialogue window it is possible to configure filtering of the data packages based on the source and target MAC addresses.

Only data packages provided with a source and/or target MAC address are admitted or filtered. Via the Protocol setting, it is possible to further restrict the data packages specifically.

The **source MAC address** defines the participant MAC address that sends in the data. The **target MAC address** defines the participant MAC address that is meant to receive the data.


MAC addresses and MAC protocol of the rule
Source MAC address:
Use hardware groups
Destination MAC address:
Use hardware groups
Protocol:
==
*
Back
Next
Here you can set the MAC address and the protocol of the packets that should be matched by the rule. A MAC address identifies a network adapter uniquely.
Example: 00:01:EE:FF:0C:42
Instead of using single MAC addresses, you may use groups of them, if you have previously defined them on the hardware groups page.
ARP
(Address Resolution Protocol)
For address assignment and ping packets.
IP

Note:

If the "Use hardware groups" option is activated (checkbox ticked) hardware groups previously added can be selected. Please use this option if you'd like to assign rules to more than one MAC address.

Note:

Should you wish to avail of a long-term connection between two permanently defined devices, here it is possible to enter the MAC addresses of both devices respectively.

Protocol	Description
ARP	The Address Resolution Protocol (ARP) is a Netzwerkprotokoll network protocol, enbaling the assignment of network addresses to hardware addresses. Although it is not restricted to Ethernet Etehrnet and IPInternet protocols, it is practically exclusively impleemnted in connection with IP-AdressierungIP addressing on Ethernet Netzen nets.
IPV4	IPv4 (Internet Protocol Version 4), earlier simply referred to as IP, is the fourth version of the Internet Protocols IP internet protocol. It was the first Internet Protocol version spread and implemented worldwide and constitutes the Internet's fundamental technical foundation Internets.
VLAN	A Virtual Local Area Network (VLAN) is a virtual local network lokales Netz within a physical network. A widespread technical implementation of VLANs has been partially defined via the IEEE IEEE 802.1Q standard provisions.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

Note:

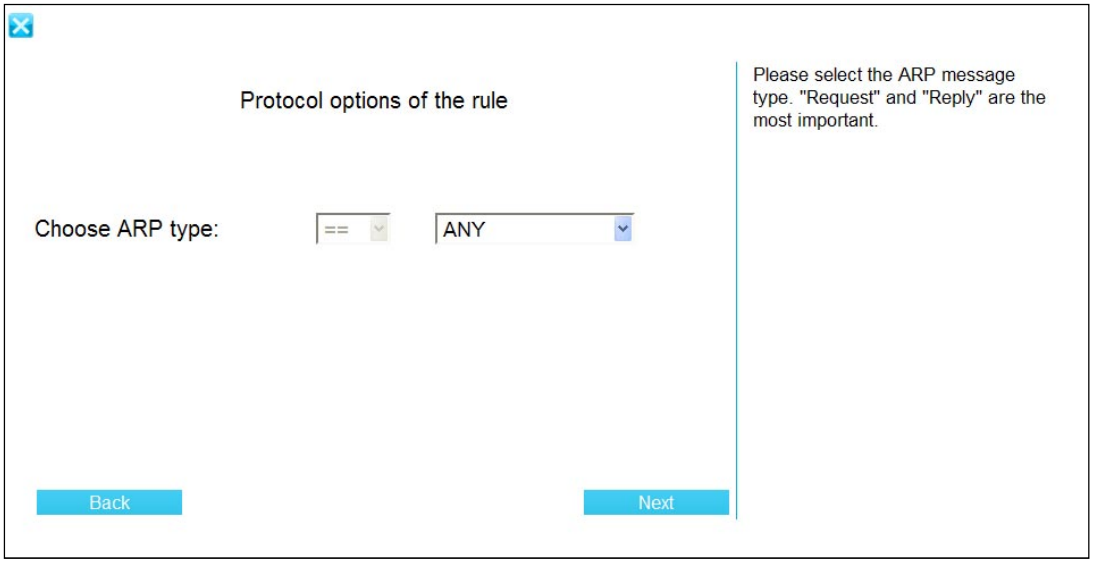
Should you not require any special protocol, select the star symbol. No further protocol settings are required and the assistant proceeds with ***Rule name and performance.***

Confirm by clicking on: ***Next***

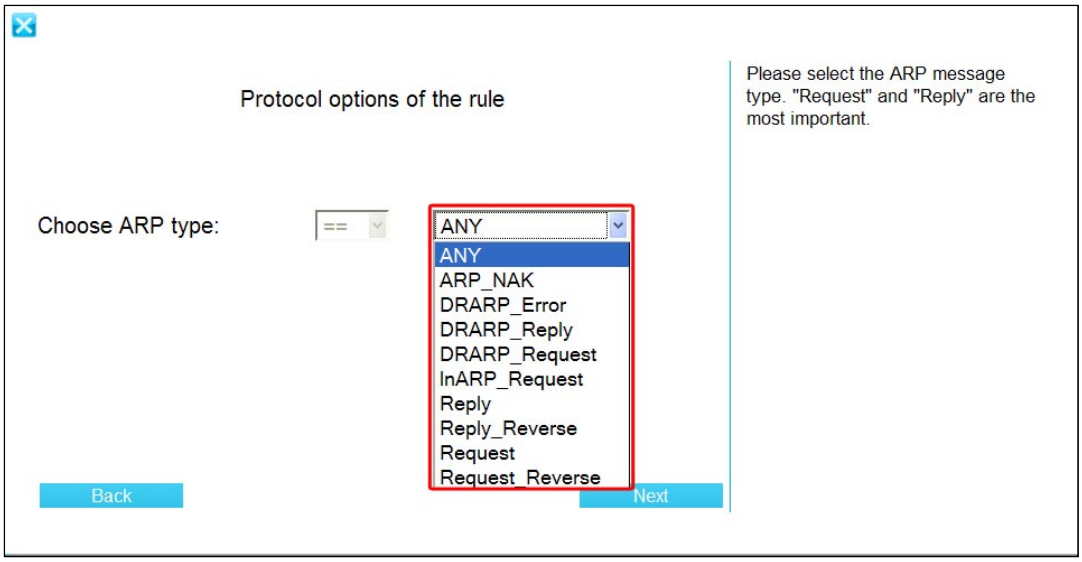
PROTOCOL OPTIONS

In the event that selection of one of the TCP, UDP or "Other" protocols has been entered, following configuration options are available:

1. ARP:

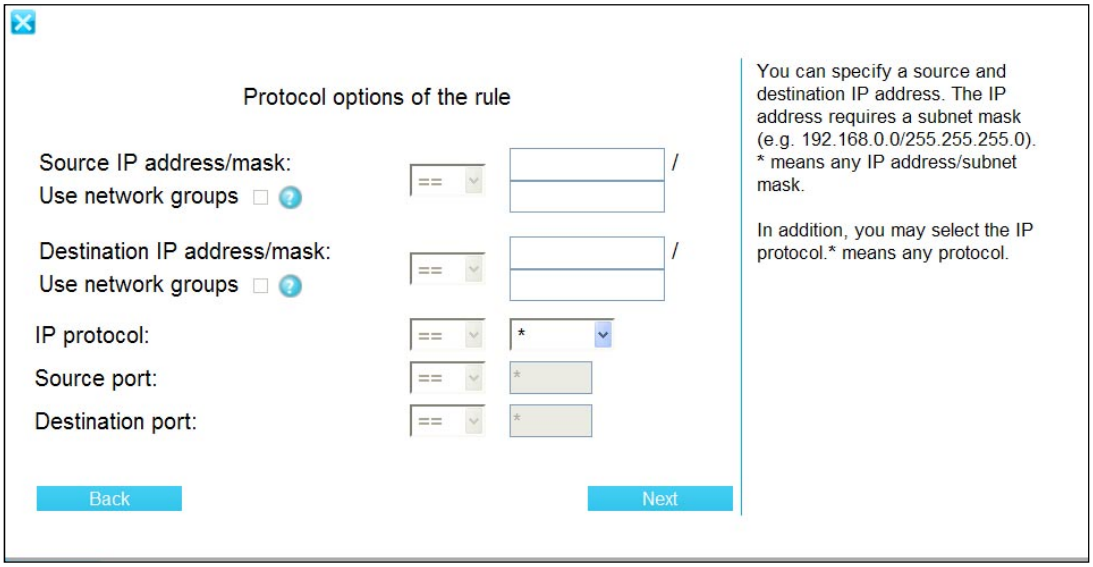


The ARP protocol allows for the following selection options:



Confirm your entries by clicking on: **Next**

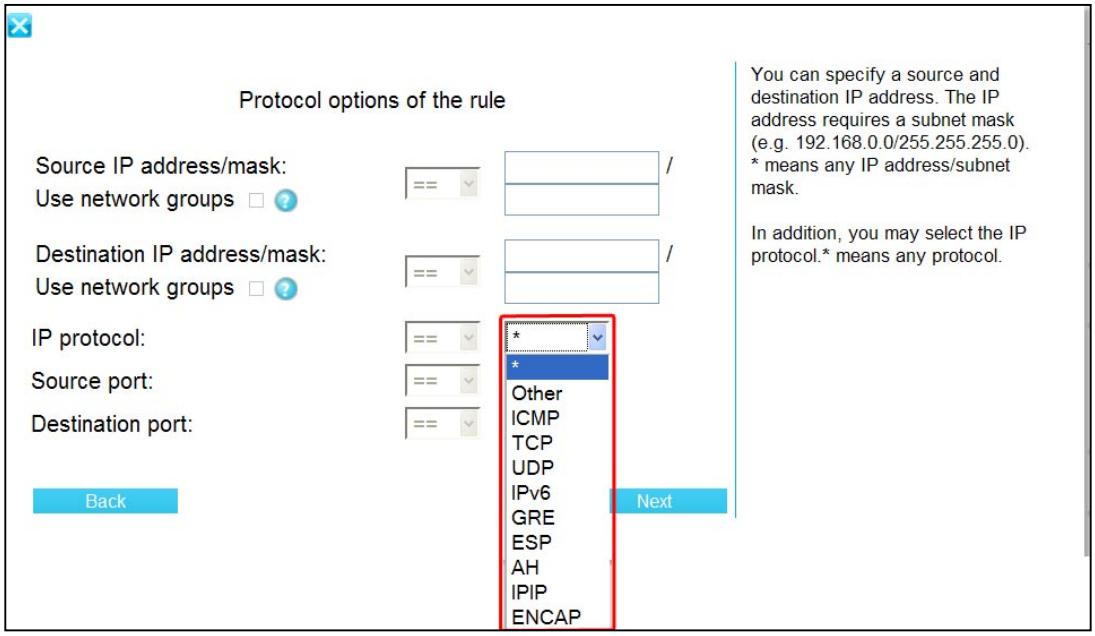
2. IPV4:


Protocol options of the rule
Source IP address/mask:
Use network groups
Destination IP address/mask:
Use network groups
IP protocol:
Source port:
Destination port:
Back
Next
You can specify a source and destination IP address. The IP address requires a subnet mask (e.g. 192.168.0.0/255.255.255.0). * means any IP address/subnet mask.
In addition, you may select the IP protocol.* means any protocol.

The IPV4 protocol provides for a further, extensive selection of filter criteria. It is possible to filter source IP addresses, target IP addresses, IP protocol, as well as source and target ports.

Note:
TCP/UDP ports may be specified as port ranges. E.g. 80:88 for 80-88, :1024 (all ports are<1024), or 1024: (all ports are above 1024)

Under IP protocol, the following protocols (*in the red text box*) are available for selection:



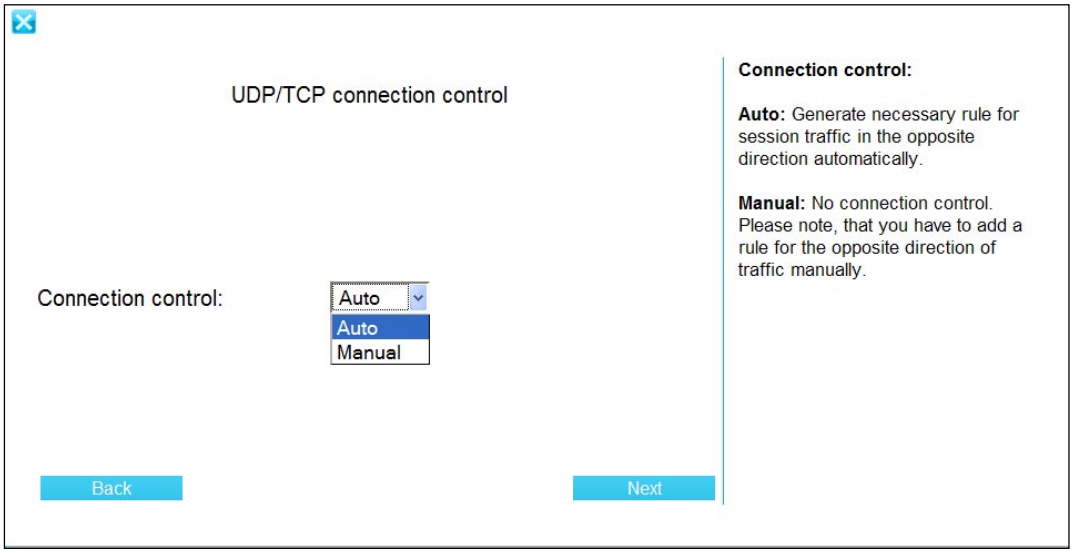
Confirm your entries by clicking on: **Next**

Should you select "Other", UDP or TCP it is necessary to proceed with some additional settings.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

UDP with IPv4:

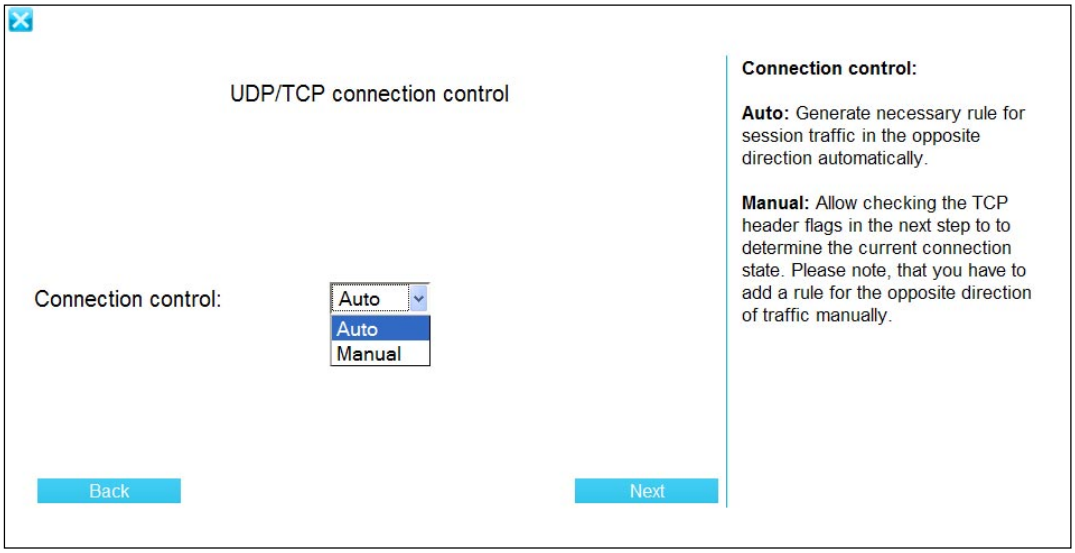
Under UDP it is necessary to select the connection control:


UDP/TCP connection control
Connection control:
Auto
Auto
Manual
Back
Next
Connection control:
Auto: Generate necessary rule for session traffic in the opposite direction automatically.
Manual: No connection control. Please note, that you have to add a rule for the opposite direction of traffic manually.

Confirm your entries by clicking on: **Next**

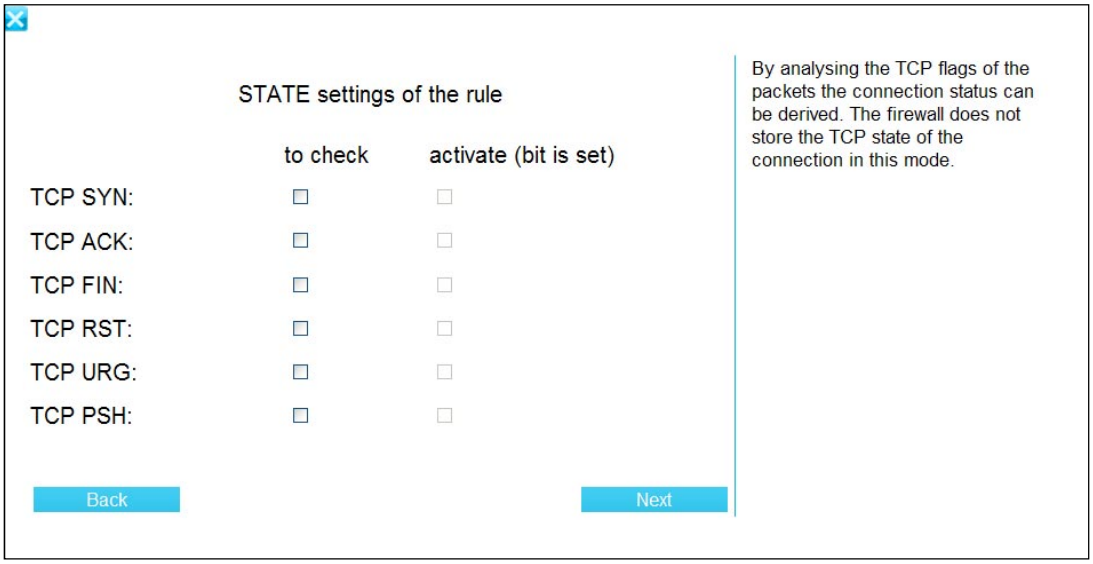
TCP under IPv4:

Under TCP it is necessary to select the connection control and with manual selection, it is necessary to set the STATE settings:


UDP/TCP connection control
Connection control:
Auto
Auto
Manual
Back
Next
Connection control:
Auto: Generate necessary rule for session traffic in the opposite direction automatically.
Manual: Allow checking the TCP header flags in the next step to to determine the current connection state. Please note, that you have to add a rule for the opposite direction of traffic manually.

Confirm your entries by clicking on: **Next**

Manual Selection:


STATE settings of the rule
to check
activate (bit is set)
TCP SYN:
TCP ACK:
TCP FIN:
TCP RST:
TCP URG:
TCP PSH:
Back
Next
By analysing the TCP flags of the packets the connection status can be derived. The firewall does not store the TCP state of the connection in this mode.

Confirm your entries by clicking on: **Next**

Note:
The following protocols are supported for status based filtering:

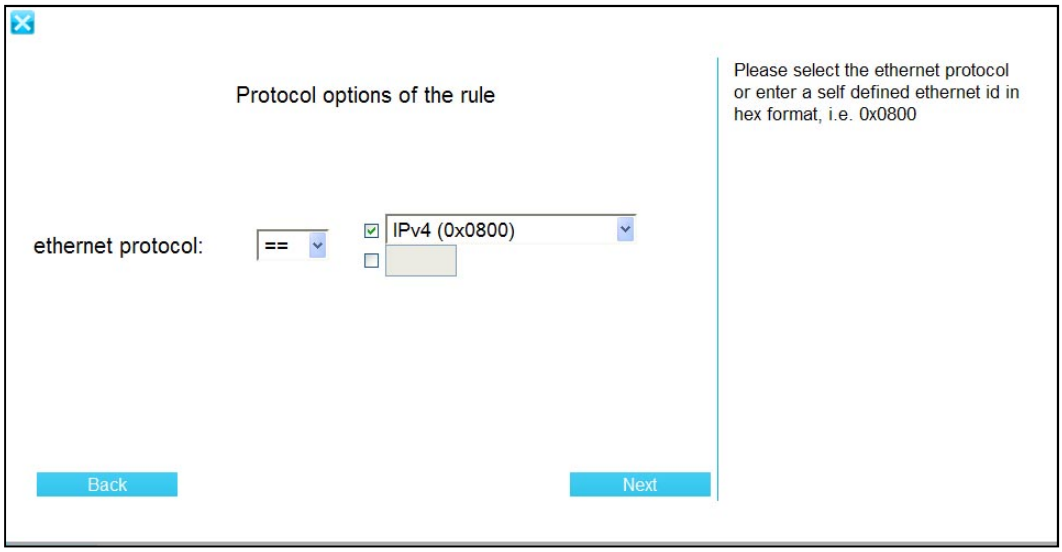
SUPPORTED FILTER BASED PROTOCOLS	
IPV4	
FTP	
TFTP	
IRC	
H323	
NETBIOS	
PPTP	
GRE	
SCTP	
RTSP	
SANE	
SIP	

Confirm your selection with: **Next**

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

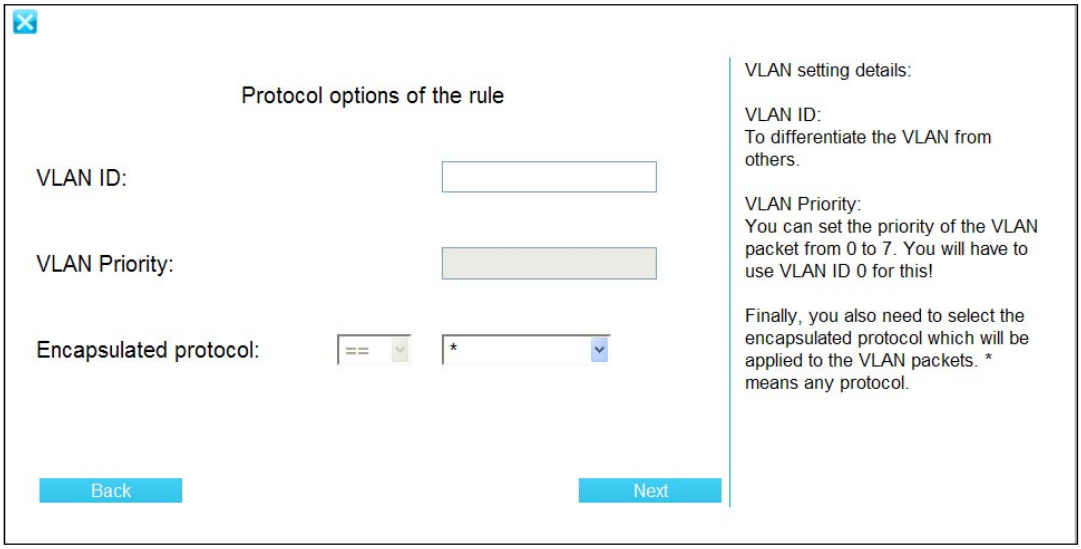
Other with IPv4:

Other lists a good number of further IP protocols for selection. It is possible to select whether implementation of a specific IP protocol is required, or whether all the IP protocols with the exception of the specified IP protocol are required.


Protocol options of the rule
Please select the ethernet protocol or enter a self defined ethernet id in hex format, i.e. 0x0800
ethernet protocol:
==
IPv4 (0x0800)
Back
Next

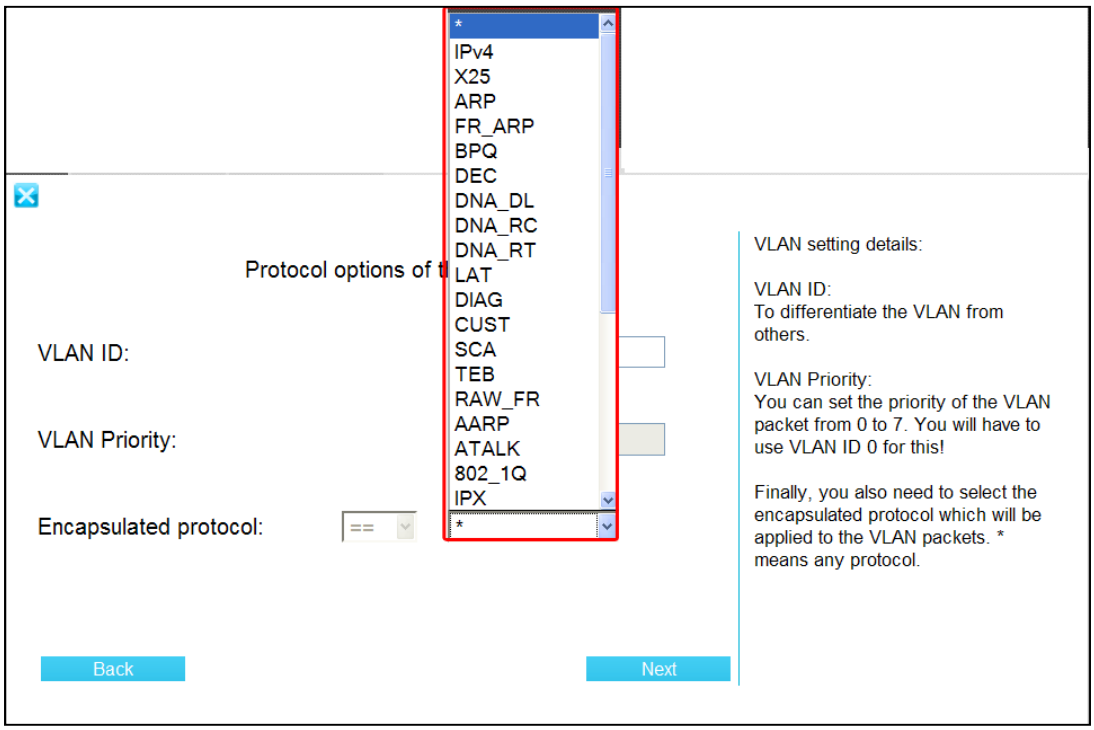
Confirm your entries by clicking on: **Next**

3. VLAN:


Protocol options of the rule
VLAN ID:
VLAN Priority:
Encapsulated protocol:
==
*
Back
Next
VLAN setting details:
VLAN ID:
To differentiate the VLAN from others.
VLAN Priority:
You can set the priority of the VLAN packet from 0 to 7. You will have to use VLAN ID 0 for this!
Finally, you also need to select the encapsulated protocol which will be applied to the VLAN packets. * means any protocol.

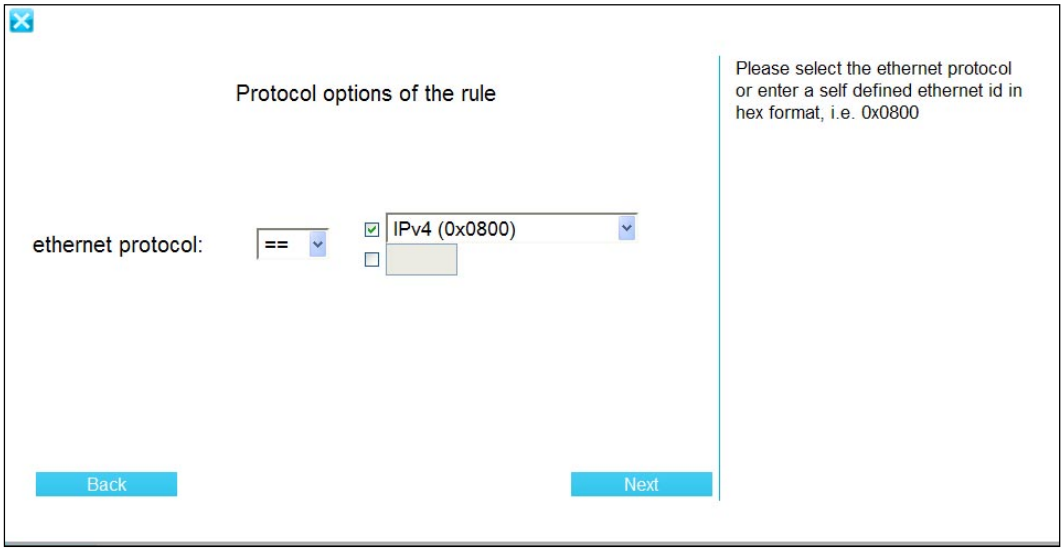
The VLAN protocol requires the entry of the VLAN ID, the VLAN Priority and the packed protocol data.

The packed protocol contains selection options of a high number of different protocol versions. It is thus possible to select whether implementation of a specific protocol is required, or whether all the protocols with the exception of the specified protocol are required.

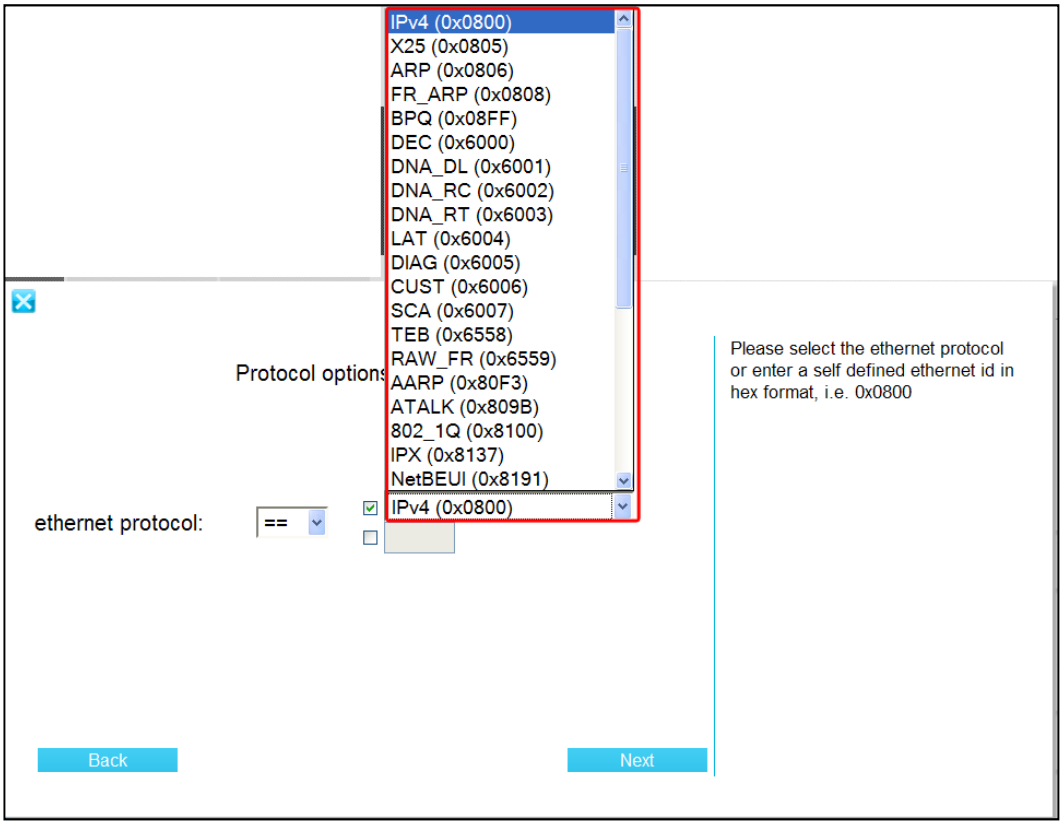


© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

4. Other:

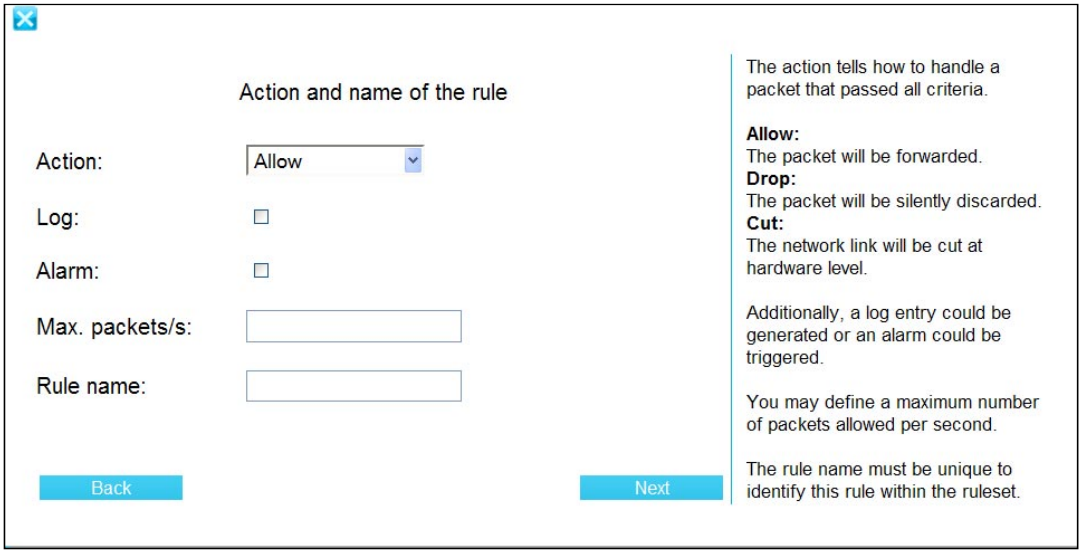

Protocol options of the rule
Please select the ethernet protocol or enter a self defined ethernet id in hex format, i.e. 0x0800
ethernet protocol:
==
IPv4 (0x0800)
Back
Next

Other includes a large number of different protocols for selection. Here you can select whether you'd like to use a specific protocol only, or if you'd like to use any but the specified protocol.



ACTION AND NAME OF THE RULE:

The dialogue window allows for the definition of rule performance: Under the **Rule Action Routine** it is possible to determine how the device is required to handle the packets: Furthermore, the events can be logged, an alarm can be set off and the data throughput / information flow rate can be restricted.


Action and name of the rule
Action:
Allow
Log:
Alarm:
Max. packets/s:
Rule name:
Back
Next
The action tells how to handle a packet that passed all criteria.
Allow:
The packet will be forwarded.
Drop:
The packet will be silently discarded.
Cut:
The network link will be cut at hardware level.
Additionally, a log entry could be generated or an alarm could be triggered.
You may define a maximum number of packets allowed per second.
The rule name must be unique to identify this rule within the ruleset.

Rule Action Routine:
Available selection here is:

Release:	The packet is forwarded.
Reject:	The packet is cancelled without notifying the sender.
Separate:	The network connection is separated (Cut) at hardware level.
Cut & Allow:	Separates data traffic between LAN-in and for ex. Service-Port.

Log:
a log entry is generated and logged.

Alarm:
The alarm output is set.

Max.Packets/sec:
Here it is possible to determine maximum number of packets per second, that can be setup as an upper limit against denial-of-service. It is anyway sensible to limit rules that in the event of frequent intervals, would generate an event log record.

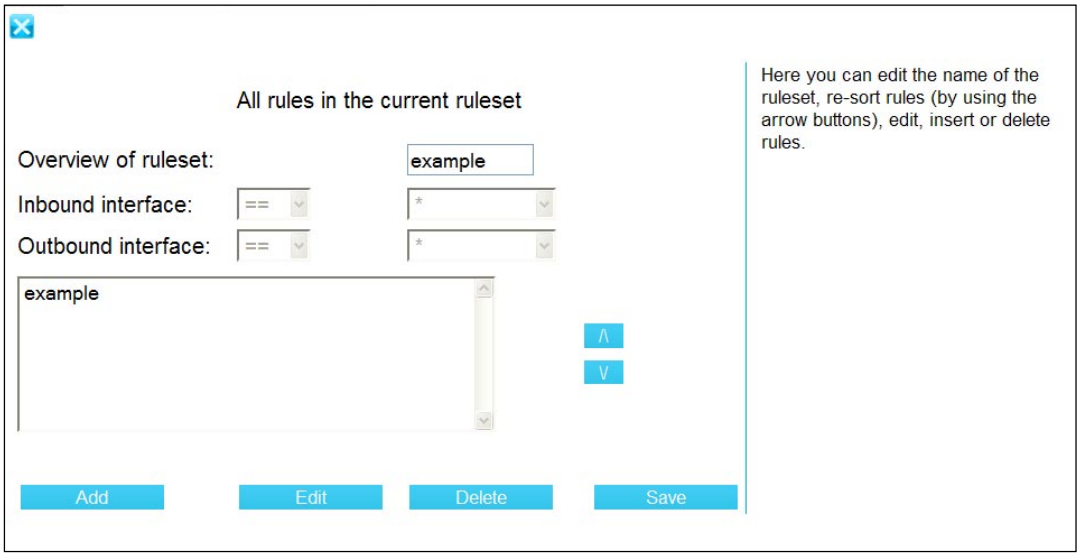
Rule Name:
Define a clear-cut, non-ambiguous rule name. It is strictly necessary that you give all the rules in the rule sets a name.

Confirm by clicking on: **Next**

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

OVERVIEW OF ALL THE RULES IN A RULE SET:

The dialogue window will display only the single rules in the rule set that can be altered in sequence. It is furthermore also possible to change the rule set name.



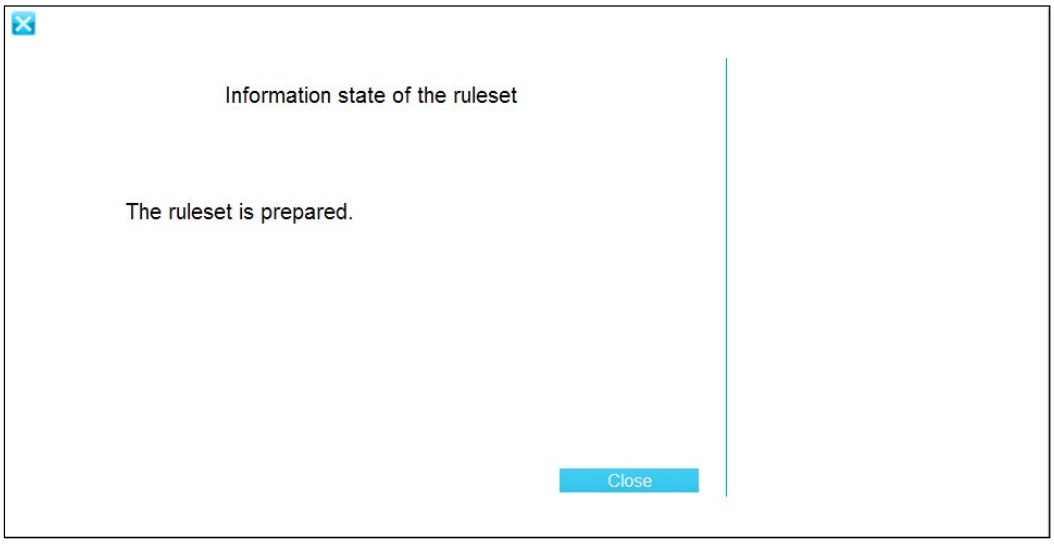
Via the **Add** button the setup process will start again and a new rule can be defined. The **Edit** button allows for the subsequent variation of rules that have already been generated.

Select Delete to remove a selected rule.

With the aid of the arrow keys it is possible to alter the position of a rule internally to a current rule set.

Confirm by clicking on: **Store**

Confirm your entries as shown on display by clicking on: **Close**





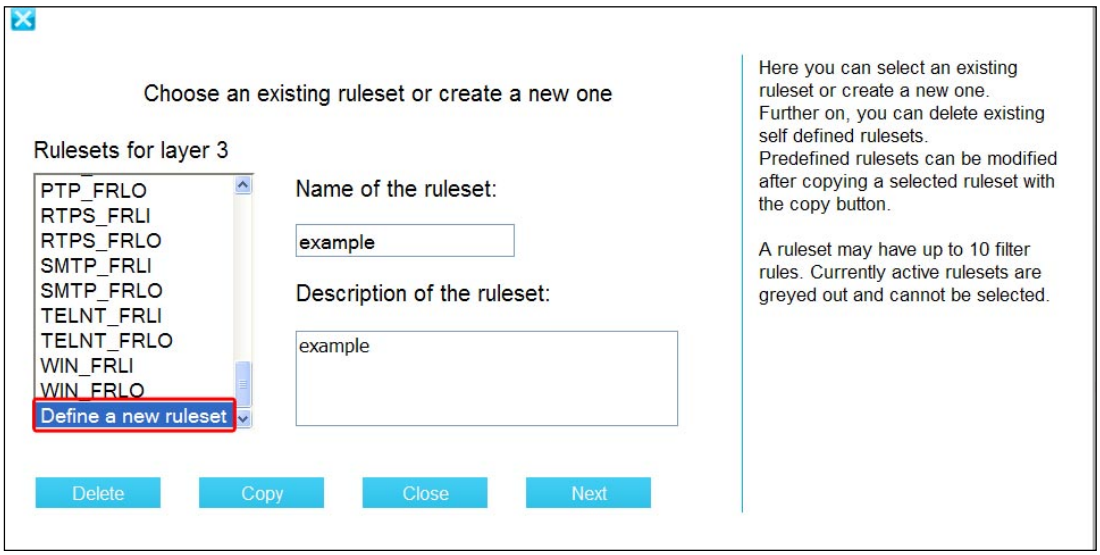
To activate the adaptations, it is necessary to run the "apply changes" function. Confirm by clicking on "**Apply settings**"..

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

7.3.5 Definition of a new rule set on Standalone IP-Interfaces (layer 3)

Note:
*Should you need to configure layer 2 filter levels, please proceed according to the **Definition of a new rule set on layer 2** section, previously herein.*

Select menu item: **Definition of a new rule set**



Enter a name and a description for the new rule set.

Note:
The rule set name is restricted to 16 characters. It is not possible to use umlauts, spaces or special characters.

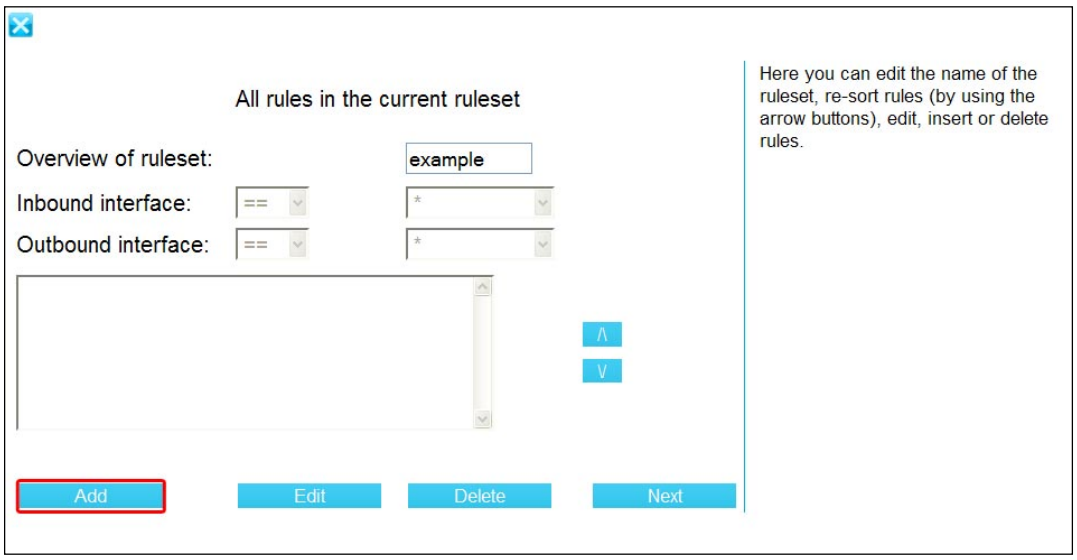
Confirm your entries by clicking on **Next**.

RULE SET LAYERS AND INTERFACES

Via the dialogue window the path of the packets on which the rule set is to be implemented, is set up. An inbound interface (via which the packets are entered) as well as an outbound interface (via which the device packets are released subsequent to acceptance) are required.

On layer 3, depending on the configuration, the following interfaces are available:

L3-VPN /Service/IPsec



Symbol description	
==	The selected interface is implemented.
!=	All interfaces are implemented, **except for** the selected interface

EXAMPLE:

Interface	Selection	Result
Inbound interface: **LAN-in**	==	filters all the inbound data packets on **LAN-in**
Outbound interface **LAN-out**	==	filters all the outbound data packets on the **LAN-out** port.

Note:

Should you not have any need to filter special ports, select the star symbol, which represents the standard settings.

Confirm your entries by clicking on: **Next**

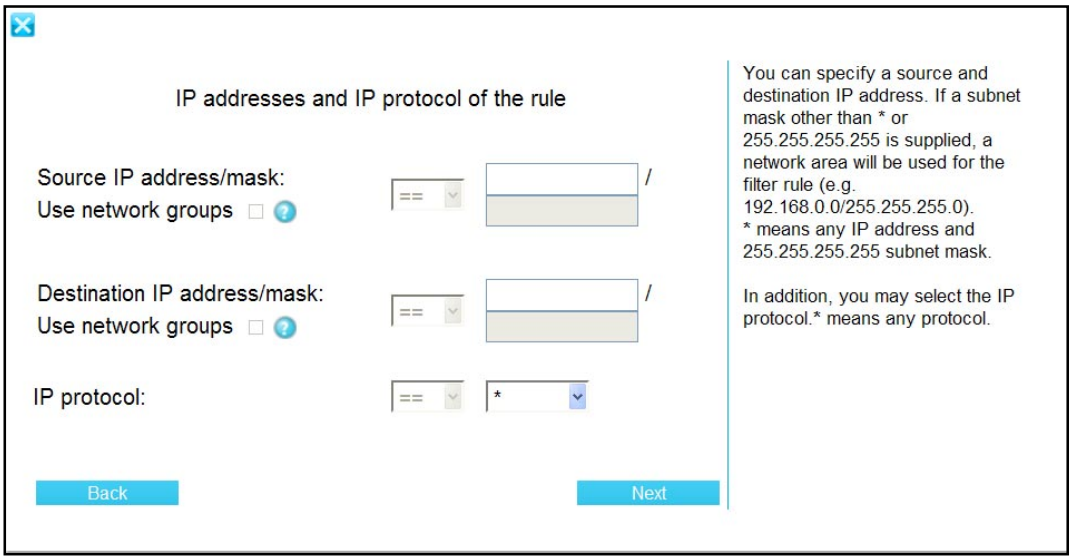
© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

RULE-RELATED IP ADRESSES AND IP PROTOCOLS

Via the dialogue window it is possibile to configure filtering of the data packages based on the source and target IP addresses.

Only data packages provided with a source and/or target IP address are admitted or filtered. Via the Protocol setting, it is possible to further restrict the data packages specifically.

The **source IP address** defines the participant IP address sending in the data. The **target IP address** defines the participant IP address that is meant to receive the data.


IP addresses and IP protocol of the rule
Source IP address/mask:
Use network groups
==
/
Destination IP address/mask:
Use network groups
==
/
IP protocol:
==
*
Back
Next
You can specify a source and destination IP address. If a subnet mask other than * or 255.255.255.255 is supplied, a network area will be used for the filter rule (e.g. 192.168.0.0/255.255.255.0). * means any IP address and 255.255.255.255 subnet mask.
In addition, you may select the IP protocol.* means any protocol.

Note:

If the "Use network groups" option is activated (checkbox ticked) network groups previously added can be selected. Please use this option if you'd like to assign rules to more than one IP address.

Note:

Should you wish to avail of a long-term connection between two permanently defined devices, here it is possible to enter the IP addresses of both devices respectively.

IP address:

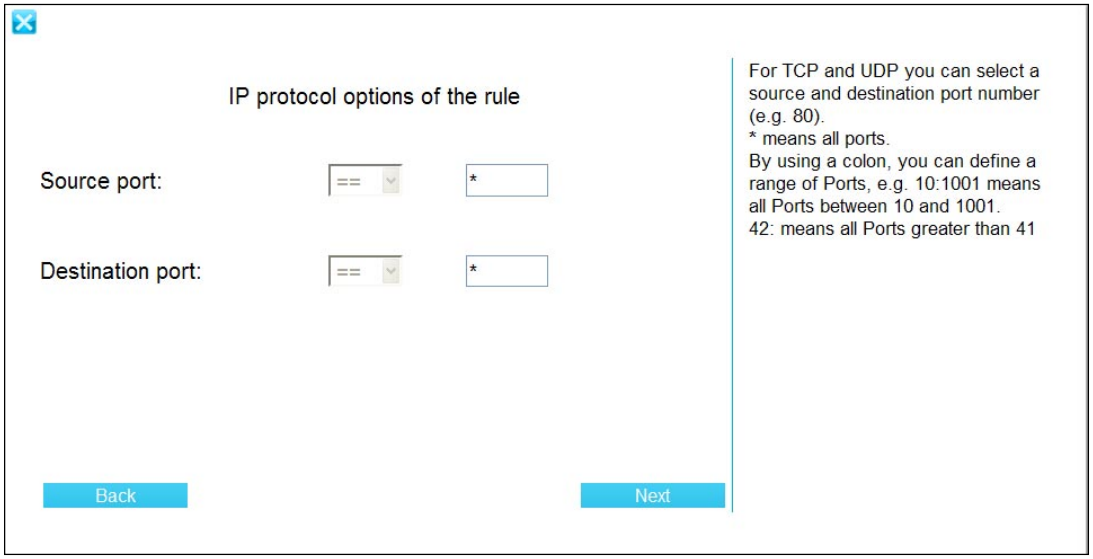
Selection	Result
TCP	The Transmission Control Protocol (TCP) is an agreement (a protocol agreement) setting forth terms and conditions for data exchange between computers. All the updated modern computer operating systems implement TCP for data exchange operations with other computers.
UDP	The User Datagram Protocol (UDP) is a minimal, connectionless net protocol belonging to the transport layers of the internet protocol families. The purpose of DTP is to accord the correct applications to the data being transferred over the internet.
ICMP	Likewise to TCP and UDP, the Internet Control Message Protocol (ICMP) also implements the Internet Protocol (IP) and is therefore part of the internet protocol families. In networks, it serves for the exchange of error and information messages.

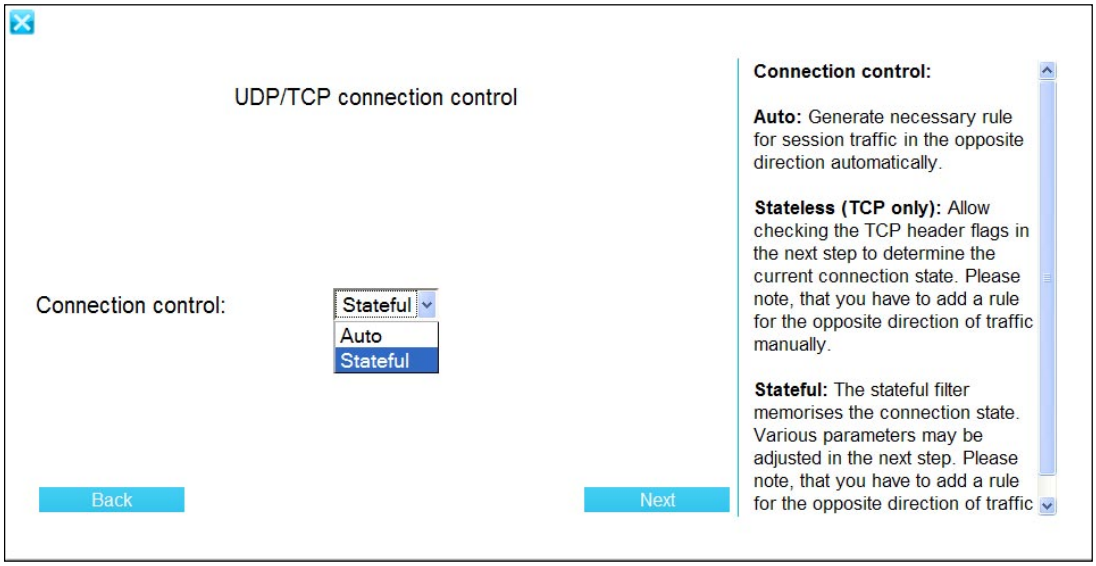
Confirm your selection by clicking on: **Next**

PROTOCOL OPTIONS

In the event that selection of one of the TCP, UDP or "Other" protocols has been entered, following configuration options are available:

1. TCP


IP protocol options of the rule
Source port:
==
*
Destination port:
==
*
Back
Next
For TCP and UDP you can select a source and destination port number (e.g. 80).
* means all ports.
By using a colon, you can define a range of Ports, e.g. 10:1001 means all Ports between 10 and 1001.
42: means all Ports greater than 41


UDP/TCP connection control
Connection control:
Stateful
Auto
Stateful
Back
Next
Connection control:
Auto: Generate necessary rule for session traffic in the opposite direction automatically.
Stateless (TCP only): Allow checking the TCP header flags in the next step to determine the current connection state. Please note, that you have to add a rule for the opposite direction of traffic manually.
Stateful: The stateful filter memorises the connection state. Various parameters may be adjusted in the next step. Please note, that you have to add a rule for the opposite direction of traffic

Auto: In TCP/UDP protocols, the back tracking of data packages is superimposed automatically. It is simply the rule link connection that needs to be specified.

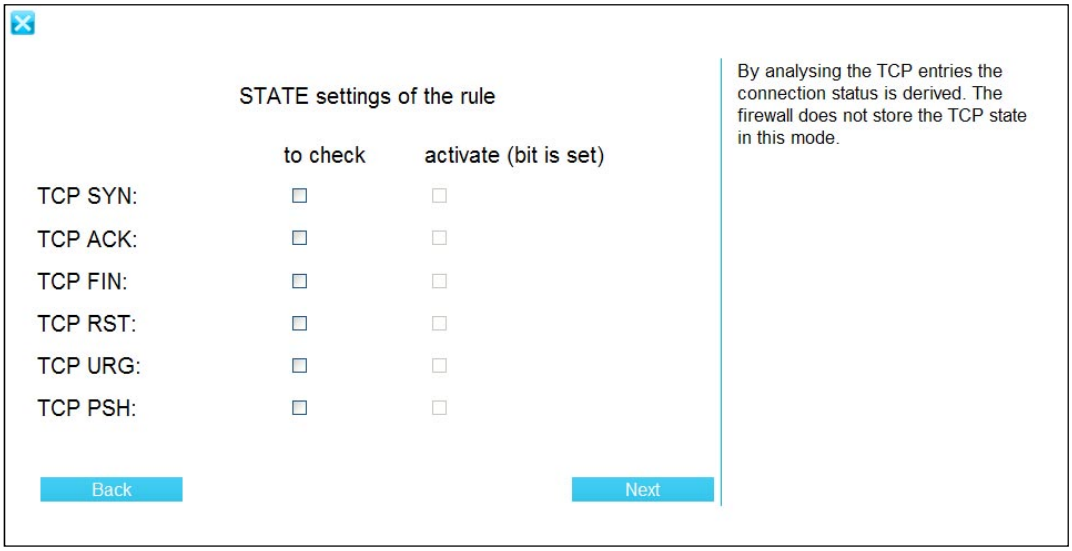
Stateless: Only for TCP:
The TCP flags such as ACK, SYN, FIN etc., can be specified manually.

Stateful: It is possible to enter various different settings such as State Related, State New, State Established and State Invalid. Manual selection of TCP flags is not possible. In this case the Firewall implements a protocol

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

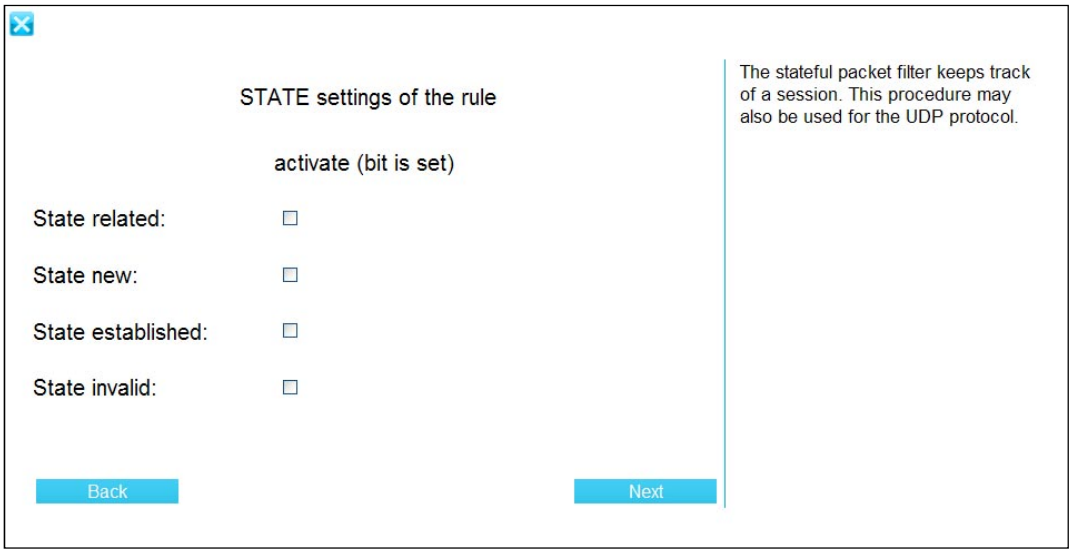
analysis for the detection of the connection conditions in a TCP connection or in a layer 6 data connection such as an FTP.

Stateless:



Confirm your selections by clicking on: **Next**

Stateful:


STATE settings of the rule
activate (bit is set)
State related:
State new:
State established:
State invalid:
Back
Next
The stateful packet filter keeps track of a session. This procedure may also be used for the UDP protocol.

State Related:	The data packet is assigned with an existing data connection, e.g. setup of an FTP feedback channel.
State New: SYN	The data package sets up a new data connection, e.g. TCP with flag.
State Established:	The data packet belongs directly to an existing data connection, e.g. TCP data without a SYN flag.
State Invalid:	Data packages for which the Firewall is not capable of determining a valid connection condition.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

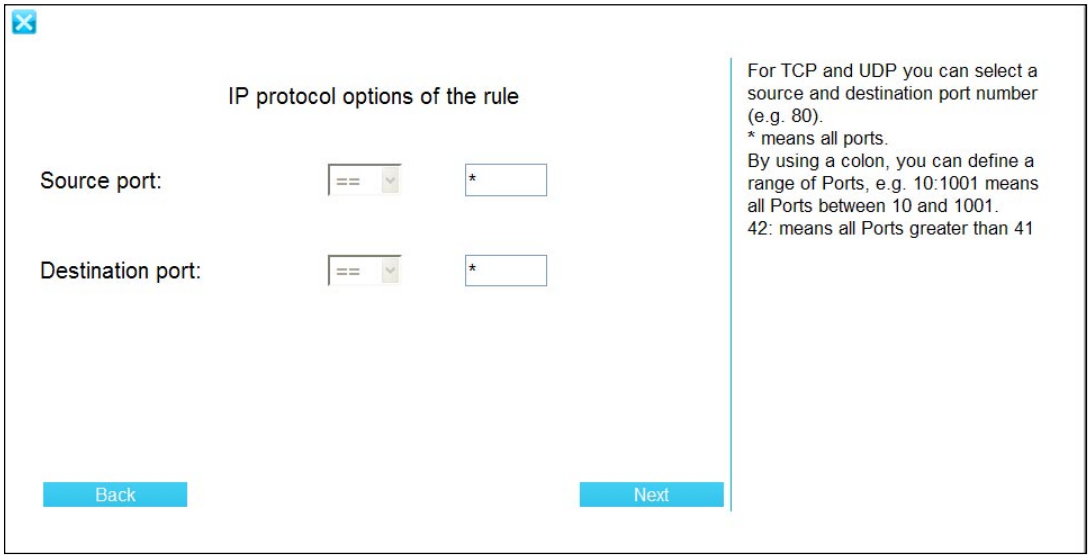
Note:
The following protocols are supported for status based filtering:

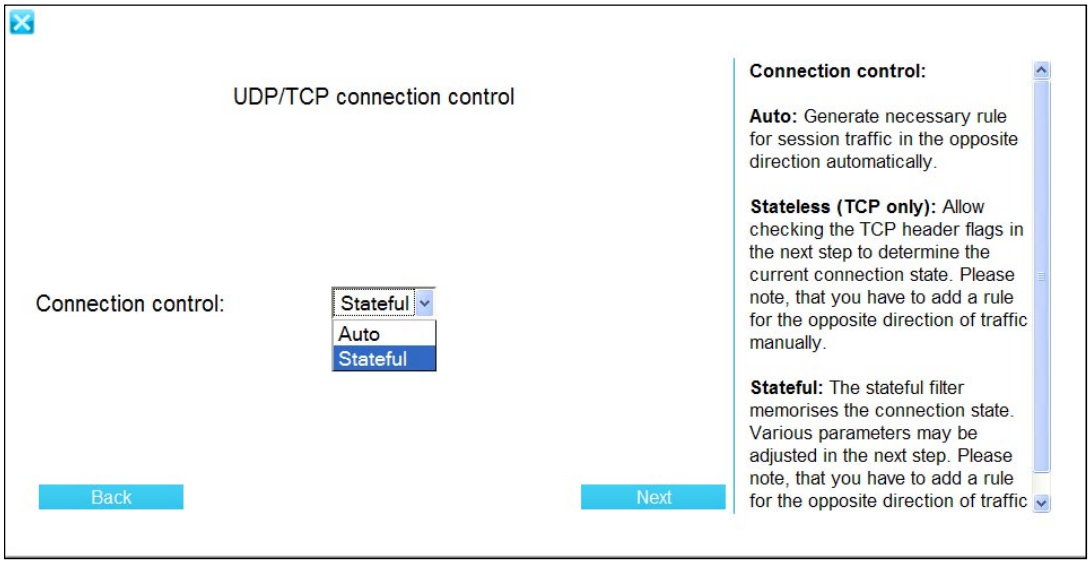
SUPPORTED FILTER BASED PROTOCOLS	
IPV4	
FTP	
TFTP	
IRC	
H323	
NETBIOS	
PPTP	
GRE	
SCTP	
RTSP	
SANE	
SIP	

Confirm your selection with: **Next**

Confirm your selections by clicking on: **Next**

2. UDP


IP protocol options of the rule
Source port:
==
*
Destination port:
==
*
Back
Next
For TCP and UDP you can select a source and destination port number (e.g. 80).
* means all ports.
By using a colon, you can define a range of Ports, e.g. 10:1001 means all Ports between 10 and 1001.
42: means all Ports greater than 41

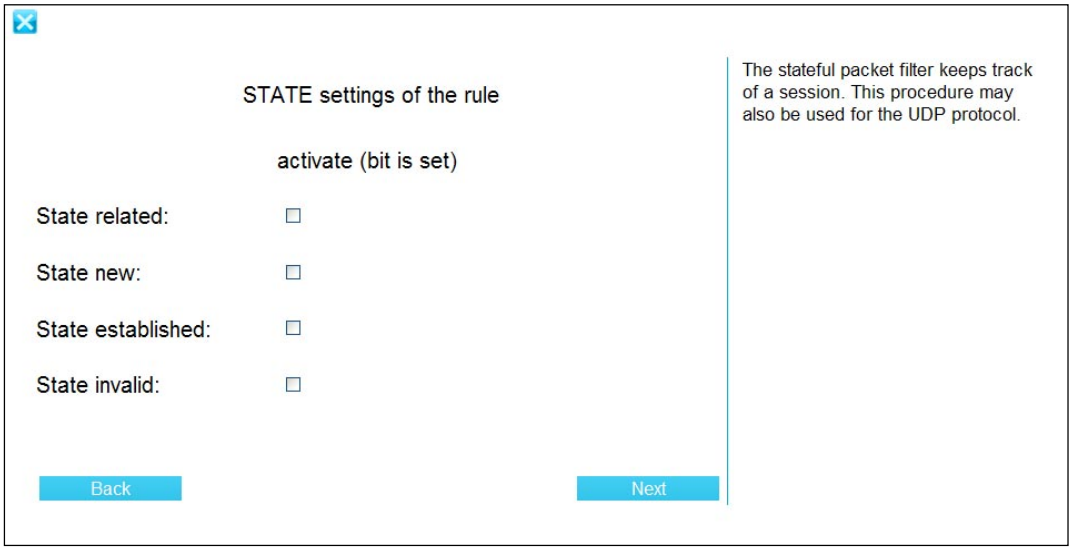

UDP/TCP connection control
Connection control:
Stateful
Auto
Stateful
Back
Next
Connection control:
Auto: Generate necessary rule for session traffic in the opposite direction automatically.
Stateless (TCP only): Allow checking the TCP header flags in the next step to determine the current connection state. Please note, that you have to add a rule for the opposite direction of traffic manually.
Stateful: The stateful filter memorises the connection state. Various parameters may be adjusted in the next step. Please note, that you have to add a rule for the opposite direction of traffic

Auto: In TCP/UDP protocols, the back tracking of data packages is superimposed automatically. It is simply the rule link connection that needs to be specified.

Stateful: It is possible to enter various different settings such as State Related, State New, State Established and State Invalid. Manual selection of TCP flags is not possible. In this case the Firewall implements a protocol analysis for the detection of the connection conditions in a TCP connection or in a layer 6 data connection such as an FTP.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

Stateful:


STATE settings of the rule
activate (bit is set)
State related:
State new:
State established:
State invalid:
Back
Next
The stateful packet filter keeps track of a session. This procedure may also be used for the UDP protocol.

State Related:	The data packet is assigned with an existing data connection, e.g. setup of an FTP feedback channel.
State New: SYN	The data package sets up a new data connection, e.g. TCP with flag.
State Established:	The data packet belongs directly to an existing data connection, e.g. TCP data without a SYN flag.
State Invalid:	Data packages for which the Firewall is not capable of determining a valid connection condition.

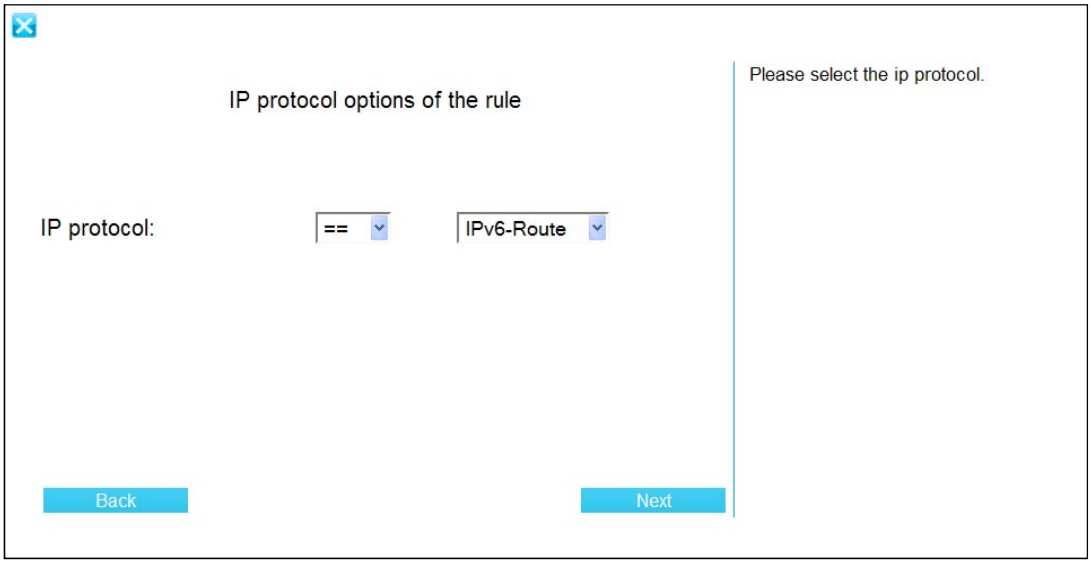
Confirm your selections by clicking on: **Next**

Note:
The following protocols are supported for status based filtering:

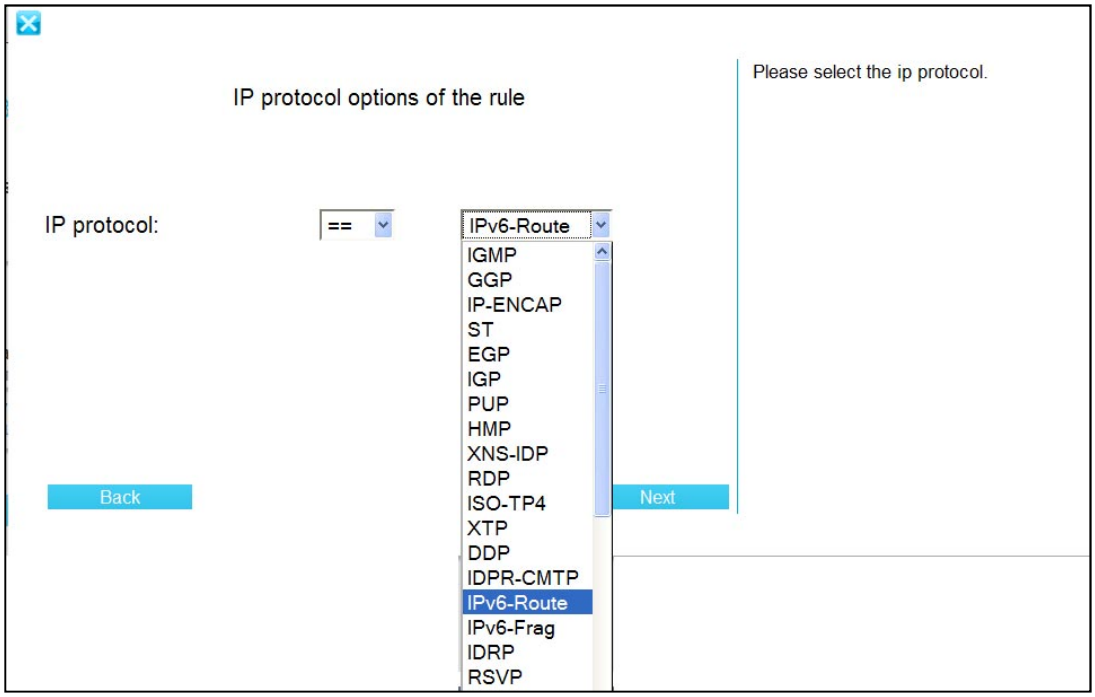
SUPPORTED FILTER BASED PROTOCOLS	
IPV4	
FTP	
TFTP	
IRC	
H323	
NETBIOS	
PPTP	
GRE	
SCTP	
RTSP	
SANE	
SIP	

Confirm your selection with: **Next**

5. Other:



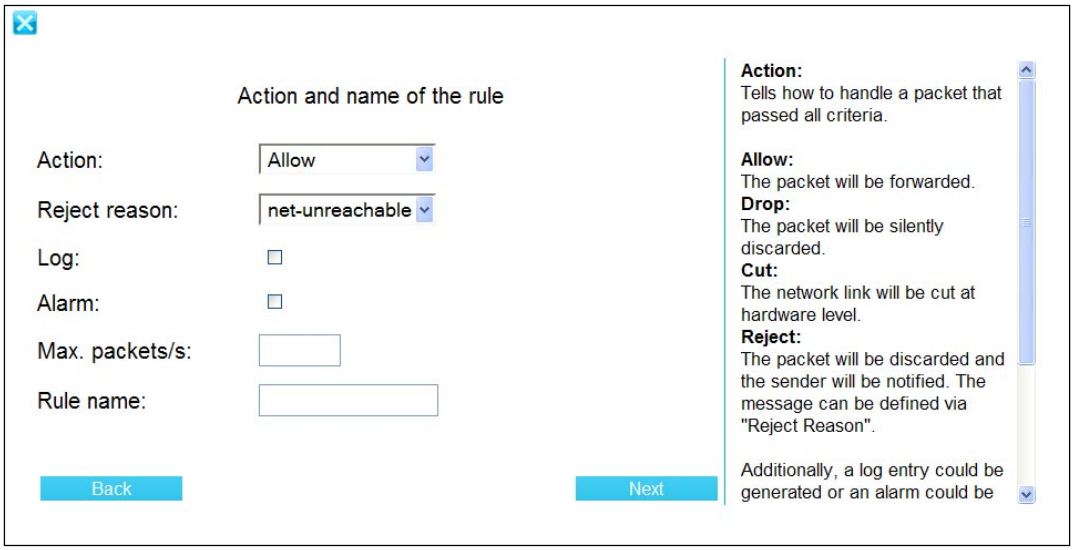
Other includes a large number of different protocols for selection. Here you can select whether you'd like to use a specific protocol only, or if you'd like to use any but the specified protocol.



© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

AKTION AND NAME OF THE RULE:

The dialogue window allows for the definition of rule performance: Under the Rule Action Routine it is possible to determine how the device is required to handle a packet. Furthermore, the events can be logged, an alarm can be set off and the data throughput / information flow rate can be restricted.



Rule Action Routine:
Available selection here is:

Release:	The packet is forwarded.
Reject:	The packet is cancelled without notifying the sender.
Separate:	The network connection is separated at hardware level.
Refuse:	The packet is cancelled and the sender is notified accordingly. It is possible to define a refusal message.
Inactive:	The rule is not implemented.
Cut & Allow:	Separates data traffic between LAN-in and for ex. Service-Port.

Reasons for refusal:
Here it is possible to define a refusal message that is then notified to the sender.

Log:
An event log entry is generated and logged.

Alarm:
The alarm output is set.

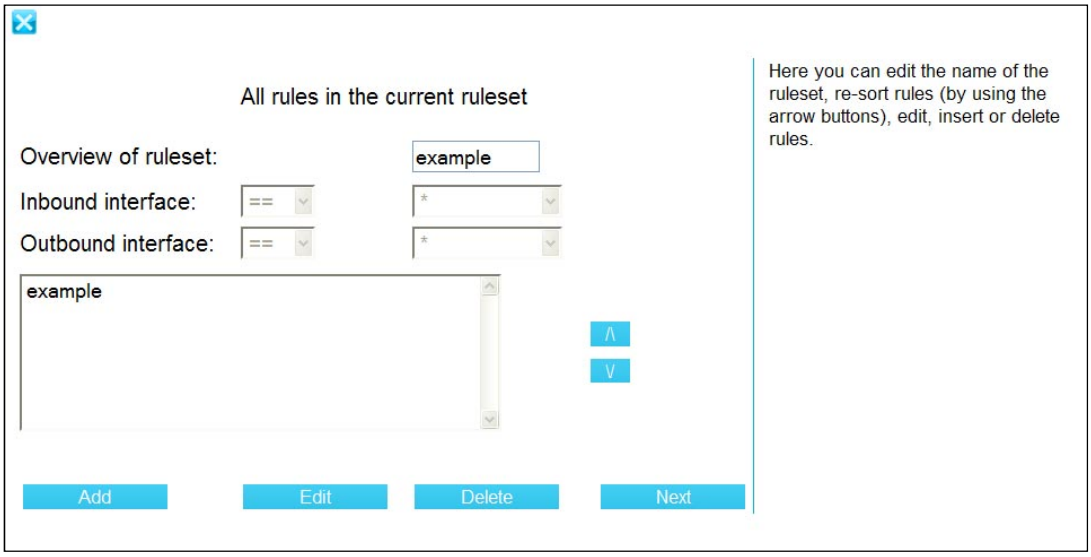
Max.Packets/sec:
Here it is possible to determine maximum number of packets per second, that can be setup as an upper limit against denial-of-service. It is anyway sensible to limit rules that in the event of frequent intervals, would generate an event log record.

Rule Name:
Define a clear-cut, non-ambiguous rule name. It is strictly necessary that you give all the rules in the rule sets a name.

Confirm by clicking on: **Next**

OVERVIEW OF ALL THE RULES IN A RULE SET:

The dialogue window displays the individual rules in a rule set. The sequence of said rules can be subject to alterations. It is furthermore also possible to change the rule set name.



Via the **Add** button the setup process will start again and a new rule can be defined. The **Edit** button allows for the subsequent variation of rules that have already been generated.

Select Delete to remove a selected rule.

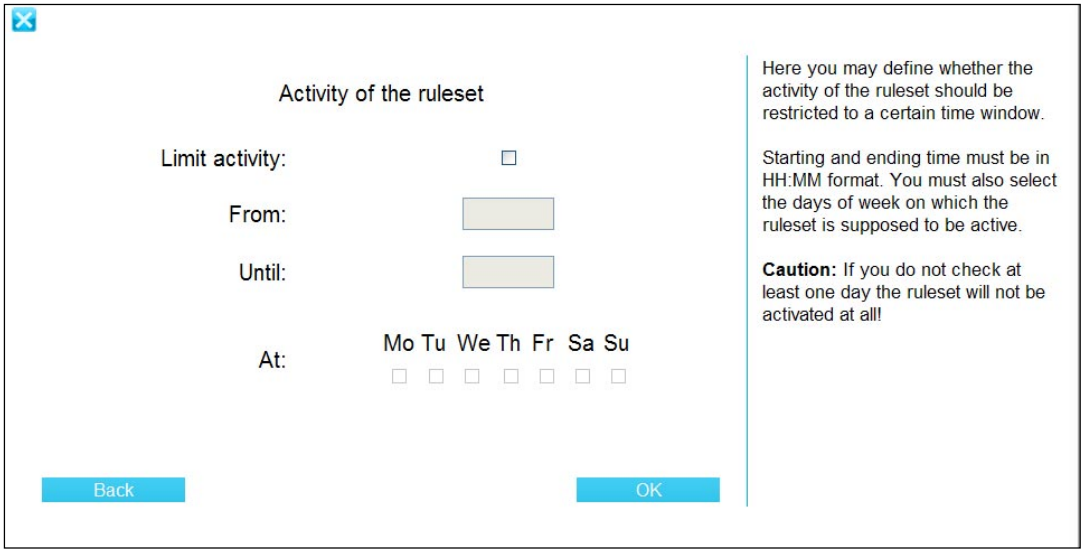
With the aid of the arrow keys it is possible to alter the position of a rule internally to a current rule set.

Confirm by clicking on: **Next**

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

RULE SET TIME SETTINGS

Via the dialogue window it is possible to enter time settings for the overall rule expression. If relative validity is restricted, it is necessary to enter a start and end time in HH:MM format. Furthermore, it is also necessary to indicate the day the rule set must be applied to.


Activity of the ruleset
Limit activity:
From:
Until:
At:
Mo Tu We Th Fr Sa Su
Back
OK
Here you may define whether the activity of the ruleset should be restricted to a certain time window.
Starting and ending time must be in HH:MM format. You must also select the days of week on which the ruleset is supposed to be active.
Caution: If you do not check at least one day the ruleset will not be activated at all!

Note:

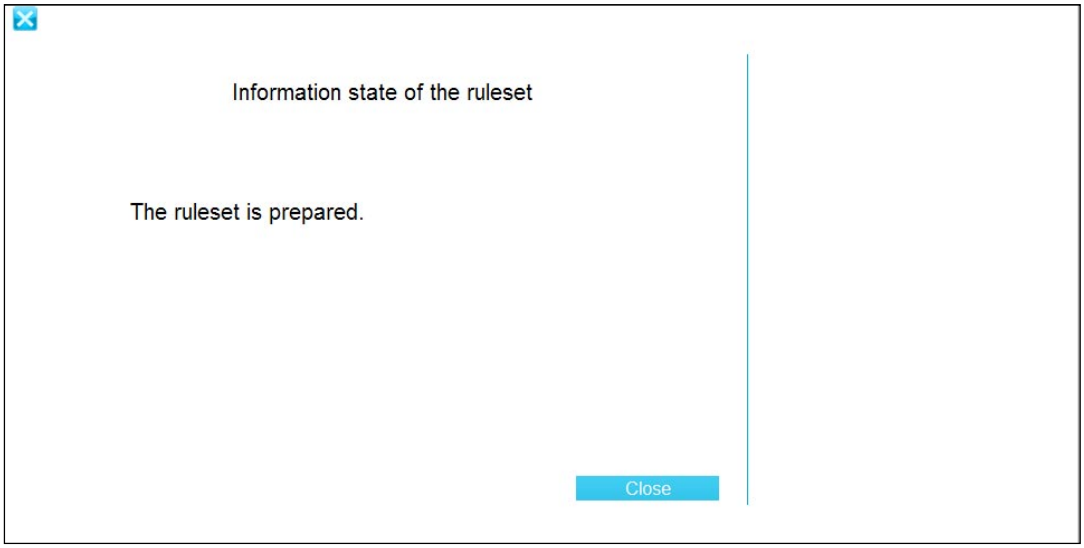
If validity is restricted at least one weekday needs to be entered, otherwise the rules are invalid and not implemented.

Note:

The validity periods must be configured considering the UTC time, regardless of which time zone might have been set up for the device!

Close configuration by clicking on **Save**.

Confirm your entries as shown on display by clicking on **Close**.



Successful selection will display the rule set in the filter overview.

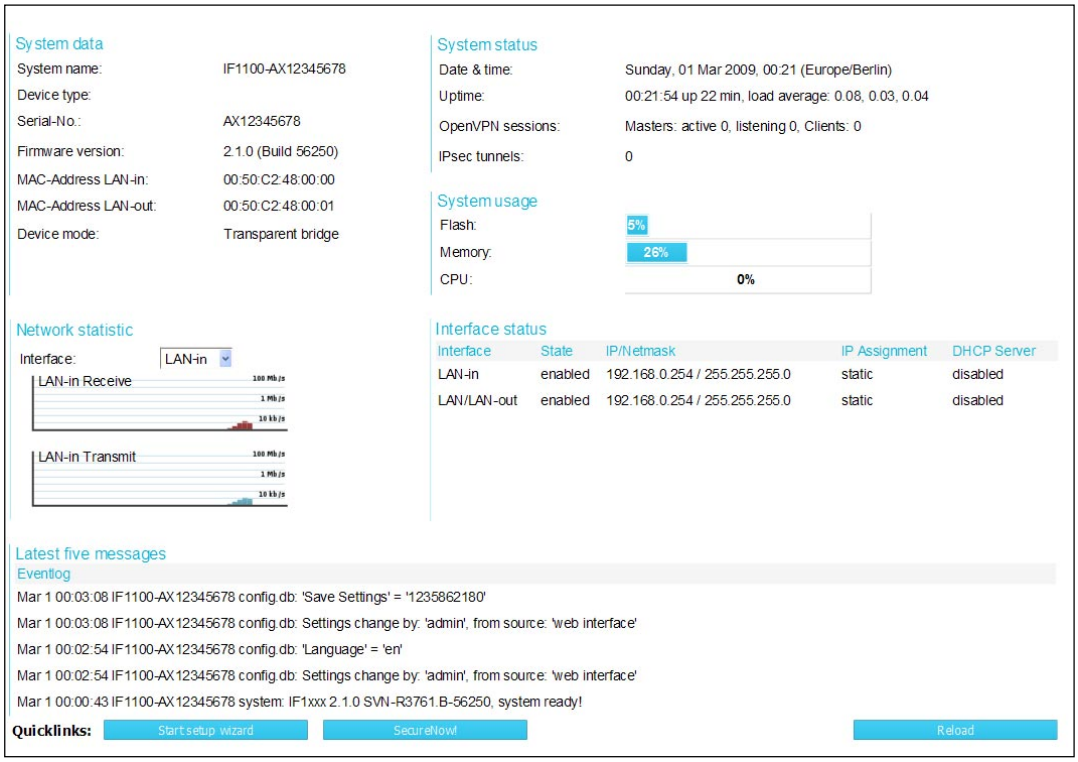


To activate the adaptations, it is necessary to run the "apply changes" function. Confirm by clicking on "**Apply settings**"..

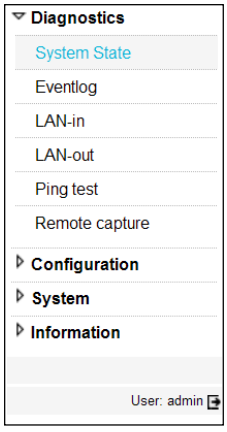
© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

8 FIREWALL WEB INTERFACE

The start page of this web interface shows important firewall parameters at a glance. Individual settings can be selected directly via hyperlink from the start page. The firewall start page is described in more detail in the system status section.


System data
System name: IF1100-AX12345678
Device type:
Serial-No.: AX12345678
Firmware version: 2.1.0 (Build 56250)
MAC-Address LAN-in: 00:50:C2:48:00:00
MAC-Address LAN-out: 00:50:C2:48:00:01
Device mode: Transparent bridge
System status
Date & time: Sunday, 01 Mar 2009, 00:21 (Europe/Berlin)
Uptime: 00:21:54 up 22 min, load average: 0.08, 0.03, 0.04
OpenVPN sessions: Masters: active 0, listening 0, Clients: 0
IPsec tunnels: 0
System usage
Flash: 5%
Memory: 26%
CPU: 0%
Network statistic
Interface: LAN-in
LAN-in Receive
LAN-in Transmit
Interface status
Interface State IP/Netmask IP Assignment DHCP Server
LAN-in enabled 192.168.0.254 / 255.255.255.0 static disabled
LAN/LAN-out enabled 192.168.0.254 / 255.255.255.0 static disabled
Latest five messages
Eventlog
Mar 1 00:03:08 IF1100-AX12345678 config.db: 'Save Settings' = '1235862180'
Mar 1 00:03:08 IF1100-AX12345678 config.db: Settings change by: 'admin', from source: 'web interface'
Mar 1 00:02:54 IF1100-AX12345678 config.db: 'Language' = 'en'
Mar 1 00:02:54 IF1100-AX12345678 config.db: Settings change by: 'admin', from source: 'web interface'
Mar 1 00:00:43 IF1100-AX12345678 system: IF1xxx 2.1.0 SVN-R3761.B-56250, system ready!
Quicklinks:
Start setup wizard
SecureNow!
Reload

The menu structure, which allows navigation through the individual configuration pages, is shown in the left part of the web interface.



DIAGNOSTICS

Shows the current interface status,

e.g.: - LAN-in
- LAN-out
- CUT & ALARM

CONFIGURATION

Configures firewall specific functions,

e.g.: - IP-Routing
- DHCP Server
- VPN

SYSTEM

Allows basic settings and changes in the web interface,

e.g.: - Software update
- Save settings

INFORMATION

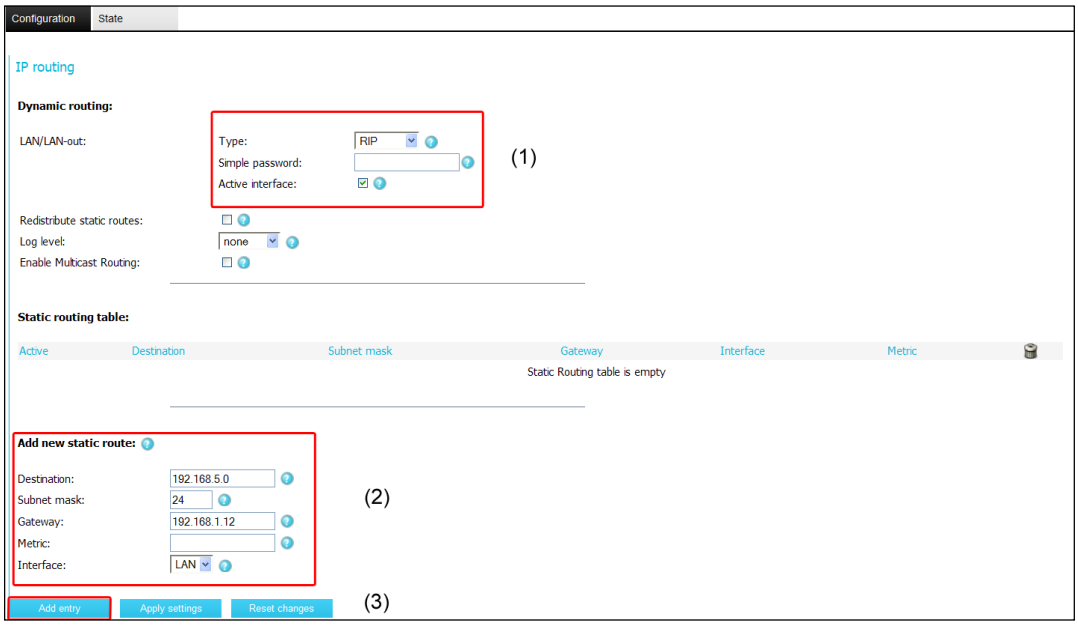
Contains general information with respect to this device,

e.g.: - Technical data
- Device installation

8.1 GENERAL OVERVIEW FOR CONFIGURATION IN THE MENUS

8.1.1 IP ROUTING EXEMPLARY CONFIGURATION

This example shows, by means of the IP routing menu item, how a setting is made and stored. Furthermore it explains how a certain setting is disabled or deleted.



Note:

If you don't know exactly, which setting is the correct one in a specific selection / input box, you can put the mouse pointer on the question mark right next to this selection. A tooltip box will appear, giving you some advice and explanation, including some examples.

SELECTION 1

Make a selection in the pull down menu first. Click on the arrow next to the setting in order to make a selection. Cinfirm with **Apply settings**.

SELECTION 2

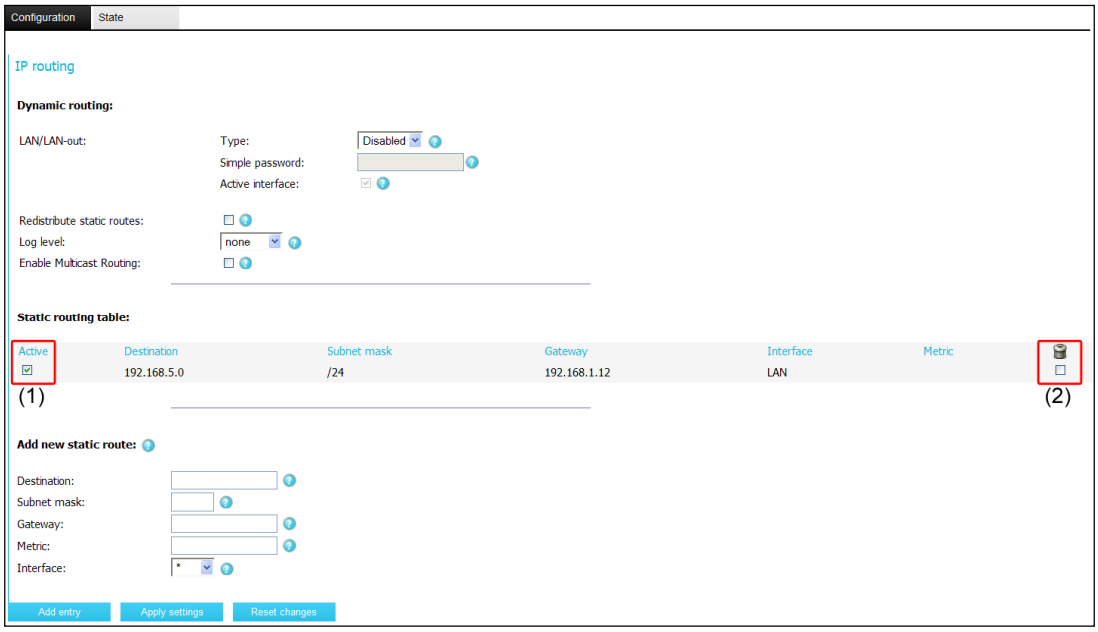
Subsequently, enter all user specific settings in the input boxes.

SELECTION 3

Confirm your entry by clicking on "**Add entry**". Your settings will now be stored.

Your settings are stored and enabled now. (Tick at no. 1)

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen



SELECTION 1

Remove the tick at no. 1 and select "**Apply settings**" if you want to disable a currently enabled setting. This setting is disabled now.

SELECTION 2

Tick the box at no. 2 and select "**Apply settings**" in order to delete a certain setting.

Note:

The "Reset changes" button in the task bar allows to reset settings you made earlier to the default value.

8.1.2 ERROR MESSAGES

The firewall identifies wrong entries by highlighting the affected input box in red.



Note:

By means of the exclamation mark next to the wrong entry you can identify what the reason for this error might be, or which values might be required.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

8.2 DIAGNOSTICS MAIN MENU ITEM

8.2.1 SYSTEM STATUS

The web interface start page shows all important firewall settings at a glance. Important Functions can be selected directly via hyperlinks from the start page.



SYSTEM DATA

The most important system data is summarised here for technical support and unambiguous firewall identification.

SYSTEM STATUS

The system status displays the current time settings used by the firewall. It is recommended to use an NTP time server in order to synchronise the local firewall time. The Uptime indicates how long the firewall runs without rebooting and also shows the load average of the system resources over this period. Furthermore, the number of optional, active VPN connections is also displayed.

SYSTEM RESOURCES

The Flash, Memory and CPU indicators represent the current load of the firewall system.

NETWORK STATISTIC

The network statistics represents the current network traffic on LAN or LAN-IN-OUT in real-time graphical form.

INTERFACE STATUS

Here you'll find an overview over the interfaces currently in use and about the status of communication ports, as well as the allocated IP addresses and subnet masks.

EVENTLOG

For faster diagnostics, the last five current event log entries will be shown in this place. You can switch to a full event log view if you use the main menu item **Eventlog** or by clicking on the **Last five messages** hyperlink.



Warning:

*Status information is statically displayed and must be refreshed via the **Reload** button on the bottom margin of the screen in the web interface or via the Reload browser function..*



Note:

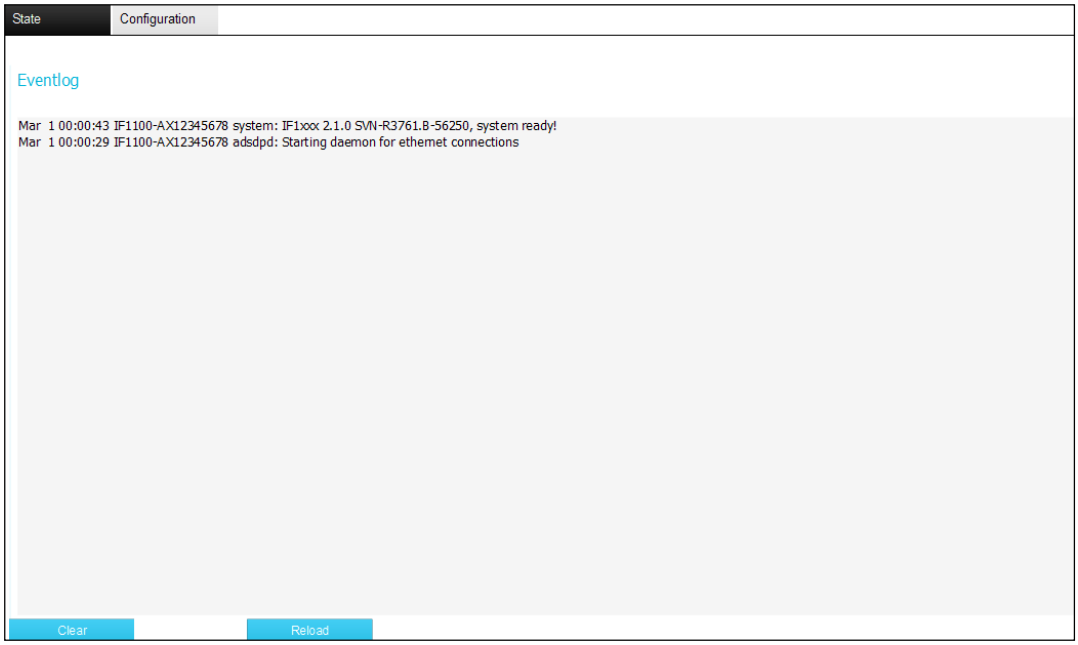
If you didn't start the setup wizard at the beginning, you can configure all settings by using several menu functions, at any point in time.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

8.2.2 EVENTLOG

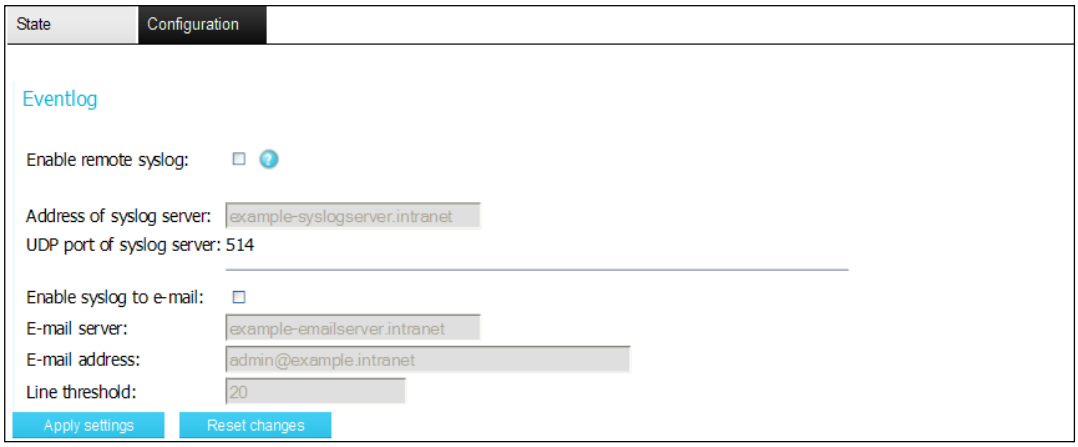
STATUS

The Eventlog represents the most important diagnostics tool of this device and contains essential information about the system status. Potential system error messages will be entered and displayed here. The Eventlog display acts like a news protocol and records all system activities. In the Eventlog, you can view changes in settings and error messages as a protocol.



CONFIGURATION

The Eventlog protocol can also conveniently be sent to a central computer. In order to do this, the remote computer will be entered in the input boxes.



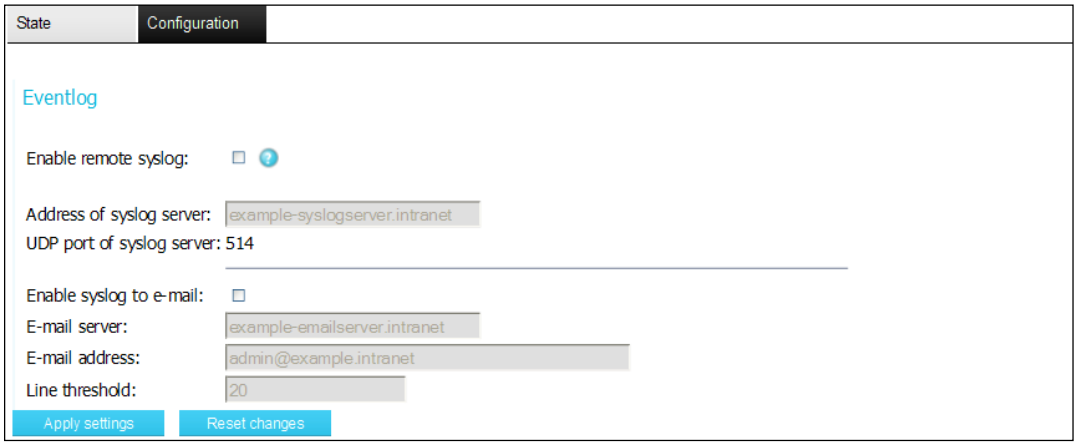
Additionally, syslog messages can be sent by email. To do this, specify the IP-address of your E-mail server and a receiver address.

Note:

In order to avoid high data volumes due to email volumes, a suitable threshold value should be entered in the Line threshold box. The Line threshold specifies the number of lines which will be sent together in one email if the threshold value is reached.

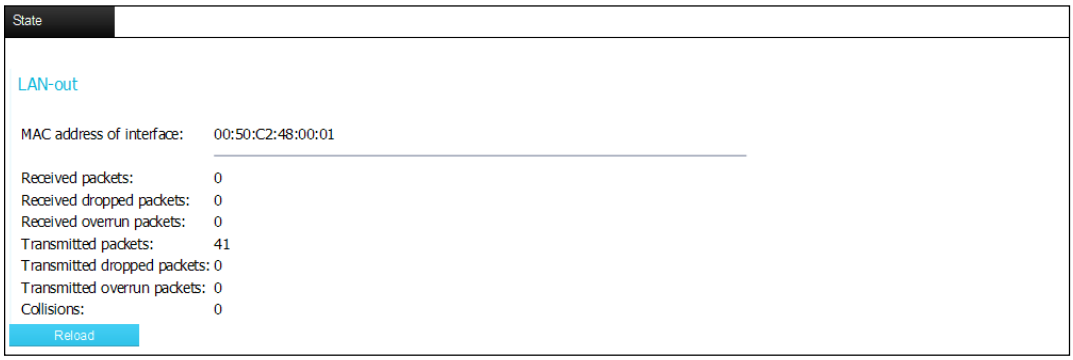
8.2.3 LAN-IN

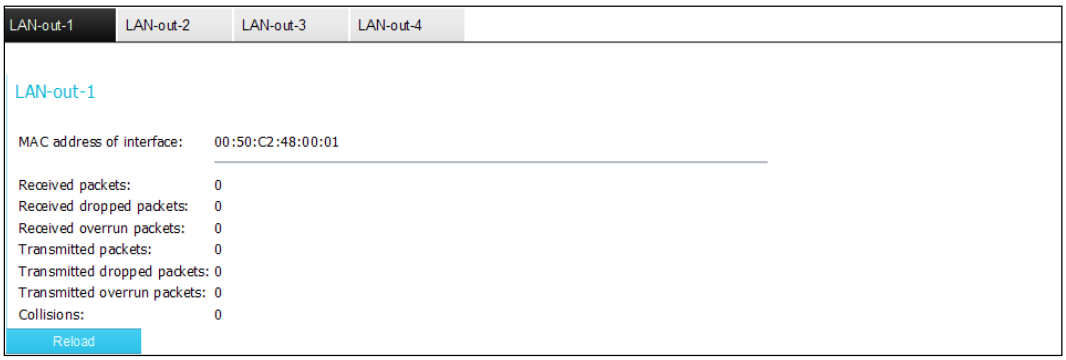
Based on the data, how the packets have been received or sent can be traced back exactly. The display can be updated by using the **Reload** button.



8.2.4 LAN-OUT

Based on the data, how the packets have been received or sent can be traced back exactly. The display can be updated by using the **Reload** button.





(Ansicht IP-Router extended LAN-out 1)

The operational mode IP-Router extended lists all four LAN-out Ports separately.

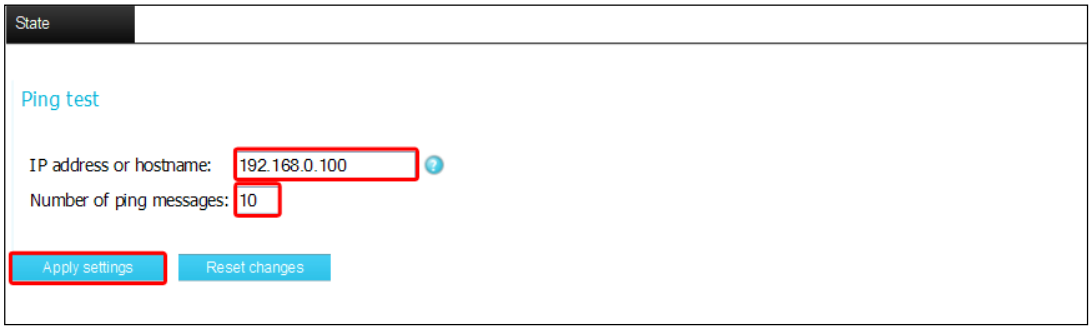
© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

8.2.5 PING TEST

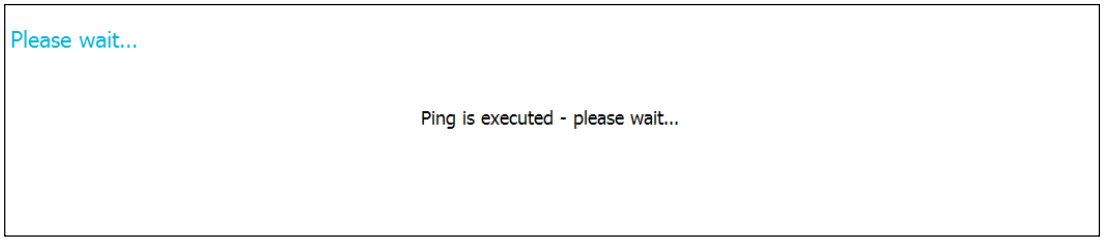
By using the Ping test option you can check if a connected remote station can be reached or not. The Ping test sends an echo request packet to the destination address of the remote station to be tested and evaluates the test information.

Please enter the destination address to be tested in form of an IP-address in the designated box. Additionally, the number of packets to be sent must be specified. It is limited to 10 packets.

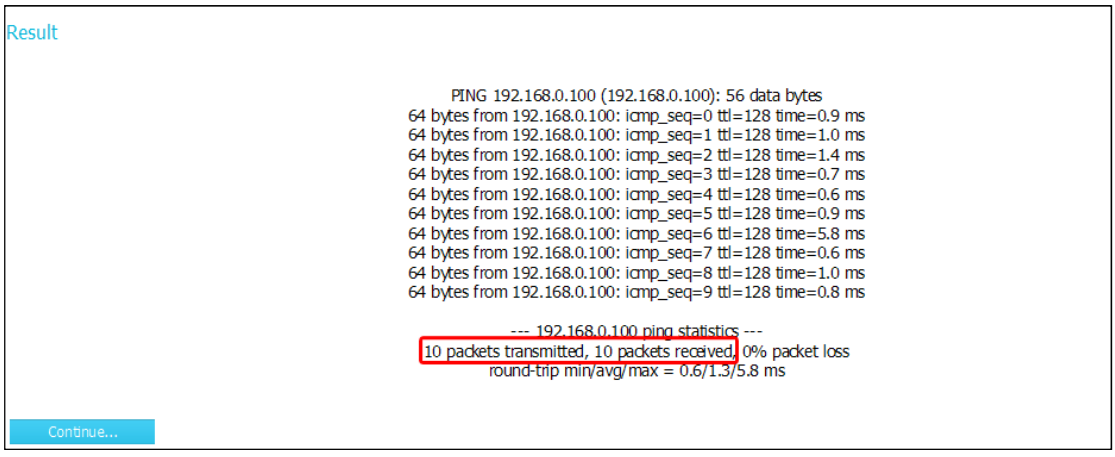
By clicking on the **Apply settings** button the ping test will start.



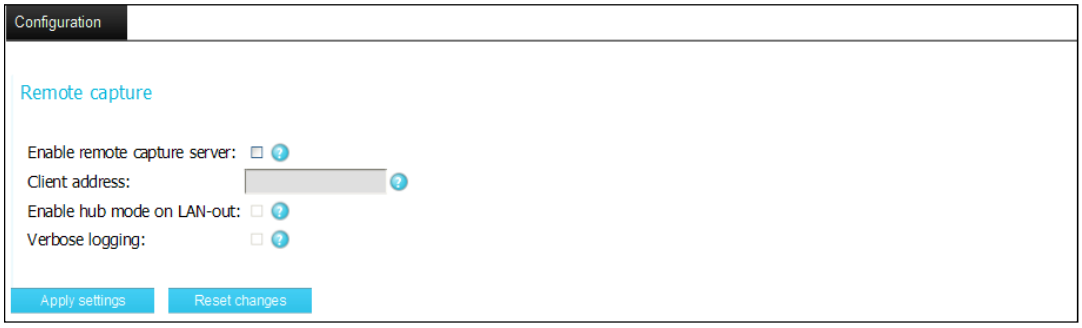
After a short time an overview will appear which shows the ping test process steps and result. The overview indicates both the sent and the received packet status.



The Ping test is finished by pressing the Continue button.


Result
PING 192.168.0.100 (192.168.0.100): 56 data bytes
64 bytes from 192.168.0.100: icmp_seq=0 ttl=128 time=0.9 ms
64 bytes from 192.168.0.100: icmp_seq=1 ttl=128 time=1.0 ms
64 bytes from 192.168.0.100: icmp_seq=2 ttl=128 time=1.4 ms
64 bytes from 192.168.0.100: icmp_seq=3 ttl=128 time=0.7 ms
64 bytes from 192.168.0.100: icmp_seq=4 ttl=128 time=0.6 ms
64 bytes from 192.168.0.100: icmp_seq=5 ttl=128 time=0.9 ms
64 bytes from 192.168.0.100: icmp_seq=6 ttl=128 time=5.8 ms
64 bytes from 192.168.0.100: icmp_seq=7 ttl=128 time=0.6 ms
64 bytes from 192.168.0.100: icmp_seq=8 ttl=128 time=1.0 ms
64 bytes from 192.168.0.100: icmp_seq=9 ttl=128 time=0.8 ms
--- 192.168.0.100 ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 0.6/1.3/5.8 ms
Continue...

8.2.6 REMOTE CAPTURE



Data packets of individual firewall interfaces can be recorded for diagnostic purposes by using the Remote Capture function. For this purpose, it is required to use the "**Wireshark**" tool in Windows. By using the **"Enable hub mode on Lan-out**" checkbox, the 4 port switch is configured in such a way that the traffic that flows between the individual Lan-out ports is also recorded.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

8.3 CONFIGURATION MAIN MENU ITEM

8.3.1 IP CONFIGURATION

The operating mode can be selected under **IP configuration**.

The following operating modes are available: Transparent bridge, IP-router and IP-router (extended).

By using the Transparent bridge mode, you can integrate the firewall into an existing network structure with no required adaptations to it. The firewall will be transparent for the existing network structure.

The firewall divides the network in two separate subnets by using IP routers. This setting may require an adaptation of the existing network structures, should it be applied.

If IP router (extended) is selected, the four ports of the LAN-out switch will be separated in four individual LAN-out ports. By separating the four IP interfaces you can, for example, operate several subnets.

All operating modes differ with respect to their configuration.

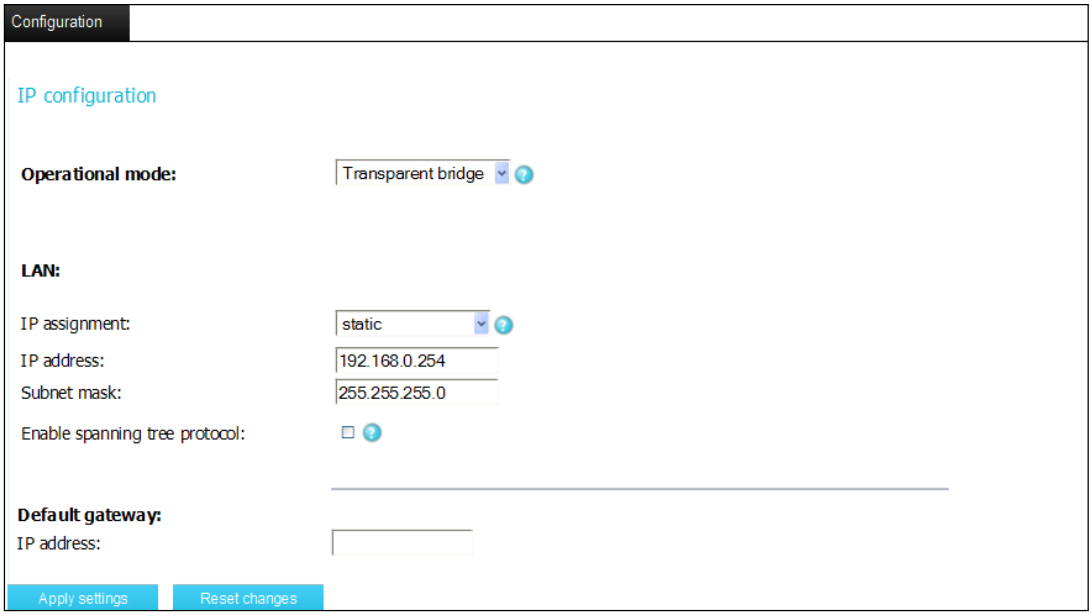
Note:

The LC display will remain blank for approx. 20 seconds if the firewall operating mode is switched from Transparent bridge mode to IP router mode and the mode is activated.

Note:

*When switching the operating mode, the device might change the MAC/IP address combination. Should you no longer be able to reach the device once the operating mode has been switched, please verify your computer's IP address and delete its ARP cache, if necessary. (Path specification under Windows: Start / Run and enter the "arp -d *" command in the command line.)*

TRANSPARENT BRIDGE



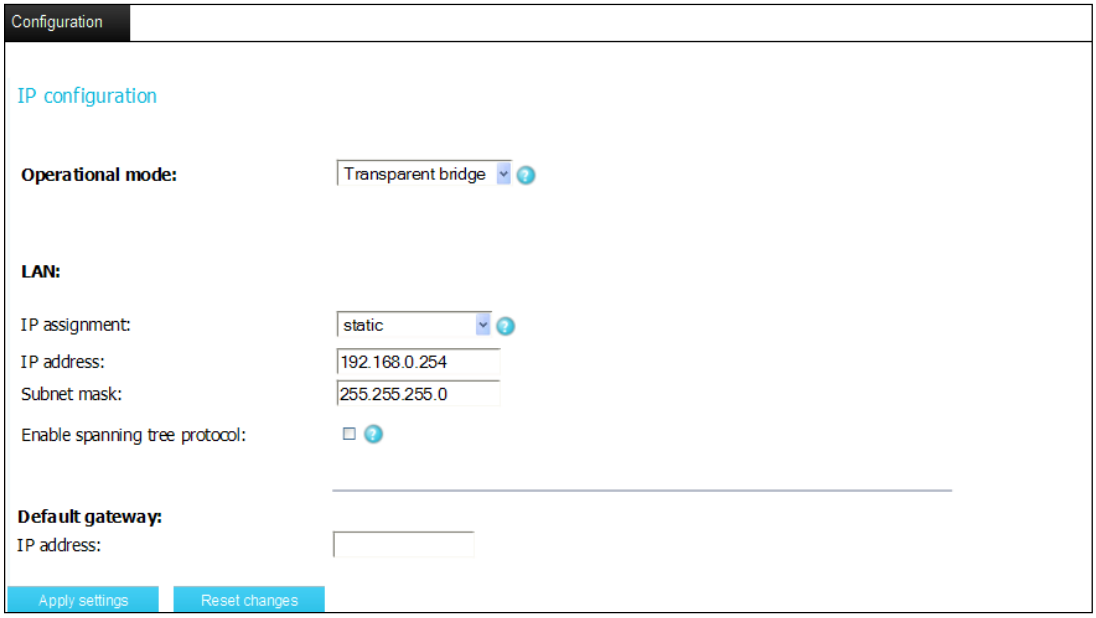
Note:

The question mark to the right of the pull down menu provides you with advice and brief explanations for the menu items available for selection.

Notes and short explanations are correctly displayed by Microsoft© Internet Explorer from version 7 and by Mozilla Firefox© browser from version 1.0.

LAN

The following pull down menu allows configuring the IP address.



Static:

If this option is selected, a permanently assigned IP address may be entered.

Static IP-address assignment requires that the IP address and the subnet mask is entered.

The default values are:

IP address: **192.168.0.254**

Subnet mask: **255.255.255.0**

DHCP:

The DHCP function requests an IP address from a DHCP server and assigns it automatically to the firewall.

DHCP with fallback address:

This option is a combination of static and automatic IP-address assignment. If an error occurs during automatic address assignment of the DHCP server or if no DHCP server is available, IP assignment automatically switches to the entered static IP address.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

PPPoE / DHCP

The IP address of the **P**oint to **P**oint **P**rotocol **o**ver **E**thernet connection is dynamically assigned by the system. This option is the classic setting for ADSL dial-up connections, in which the provider dynamically assigns the IP address.

The PPPoE user name contains the login data supplied by the provider.

Note:

Exemplary configuration for a T-Online DSL dial-up connection (without guarantee):

AAAATTTT#MMMM@t-online.de

- AAAA – 12-digit terminal identification number

- TTTT – T-Online number

- only if the T-Online number has less than twelve digits

- MMMM – user identification number

DNS via DHCP / Gateway via DHCP

If the DHCP, DHCP/Fallback or PPPoE interface is to be configured, both checkboxes will show. If several interfaces are configured on DHCP, the user decides from which of these interfaces the default gateway and DNS are to be retrieved. If only one interface is set to DHCP, the user can overwrite the values for gateway or DNS assigned per DHCP by manual configuration by clearing the checkboxes.

Note:

Every time you can only configure one interface with these options at a time. If you attempt to configure another interface, the checkboxes you had ticked in your previous configuration will be cleared.

Activate Spanning Tree Protocol:

The spanning tree protocol is used for avoiding loops in particular in network environments with switching. With this function activated, redundant network lines can be generated.

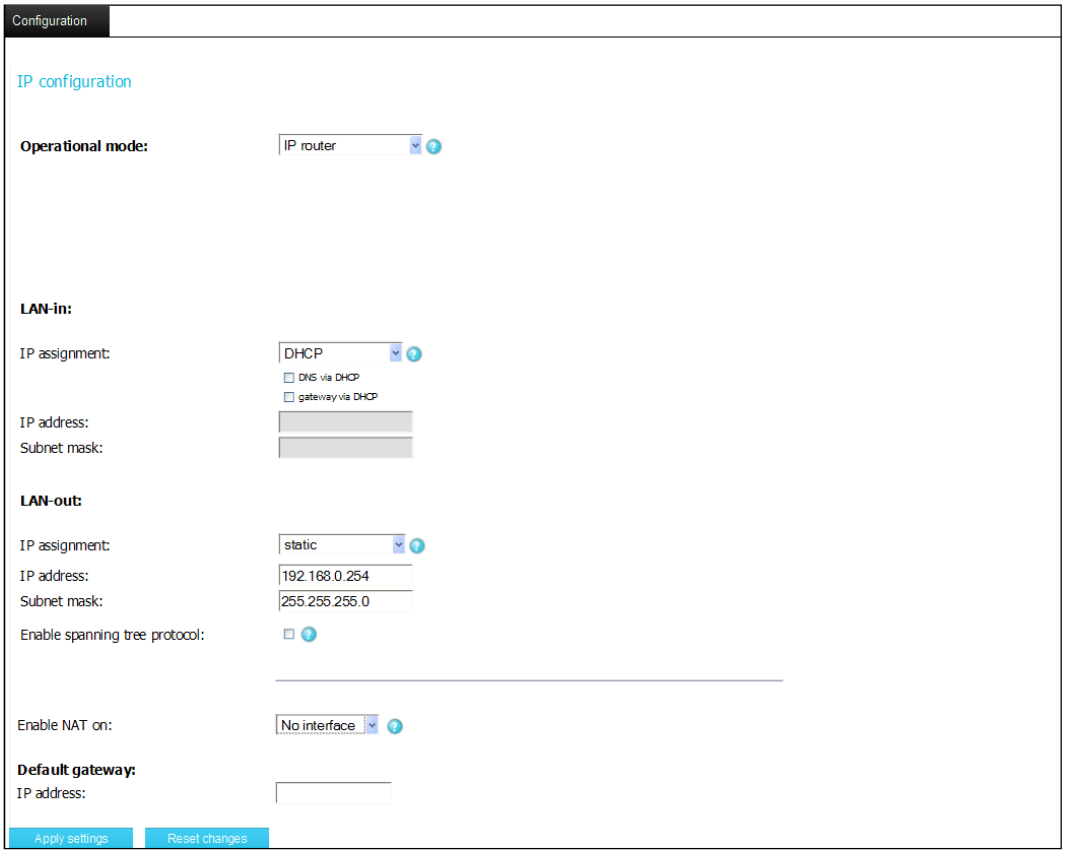
Standard gateway:

In this option, you can specify the IP address of the used gateway.

Click subsequently on: **Apply settings**

IP ROUTER

The IP router option divides the networks in two separate networks between LAN-in and LAN-out interface and filters them separately.



LAN-in/out interface:

IP assignment for the LAN-in interface can be made in two different ways:

Static:

If this option is selected, a permanently assigned IP address may be entered.

Static IP-address assignment requires that the IP address and the subnet mask is entered.

The default values are:

IP address: **192.168.0.254**

Subnet mask: **255.255.255.0**

DHCP:

The DHCP function requests an IP address from a DHCP server and assigns it automatically to the firewall.

DHCP with fallback address:

This option is a combination of static and automatic IP-address assignment. If an error occurs during automatic address assignment of the DHCP server, or if no DHCP server is available, IP assignment automatically switches to the entered static IP address.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

PPPoE / DHCP

The IP address of the **P**oint to **P**oint **P**rotocol **o**ver **E**thernet connection is dynamically assigned by the system. This option is the classic setting for ADSL dial-up connections, in which the provider dynamically assigns the IP address.

The PPPoE user name contains the login data supplied by the provider.

Note:

Exemplary configuration for a T-Online DSL dial-up connection (without guarantee):

AAAATTTT#MMMM@t-online.de

- AAAA – 12-digit terminal identification number

- TTTT – T-Online number

- only if the T-Online number has less than twelve digits

- MMMM – user identification number

DNS via DHCP / Gateway via DHCP

If the DHCP, DHCP/Fallback or PPPoE interface is to be configured, both checkboxes will show. If several interfaces are configured on DHCP, the user decides from which of these interfaces the default gateway and DNS are to be retrieved. If only one interface is set to DHCP, the user can overwrite the values for gateway or DNS assigned per DHCP by manual configuration by clearing the checkboxes.

Note:

Every time you can only configure one interface with these options at a time. If you attempt to configure another interface, the checkboxes you had ticked in your previous configuration will be cleared.

Activate Spanning Tree Protocol:

The spanning tree protocol is used for avoiding loops in particular in network environments with switching. With this function activated, redundant network lines can be generated.

Activate NAT on:

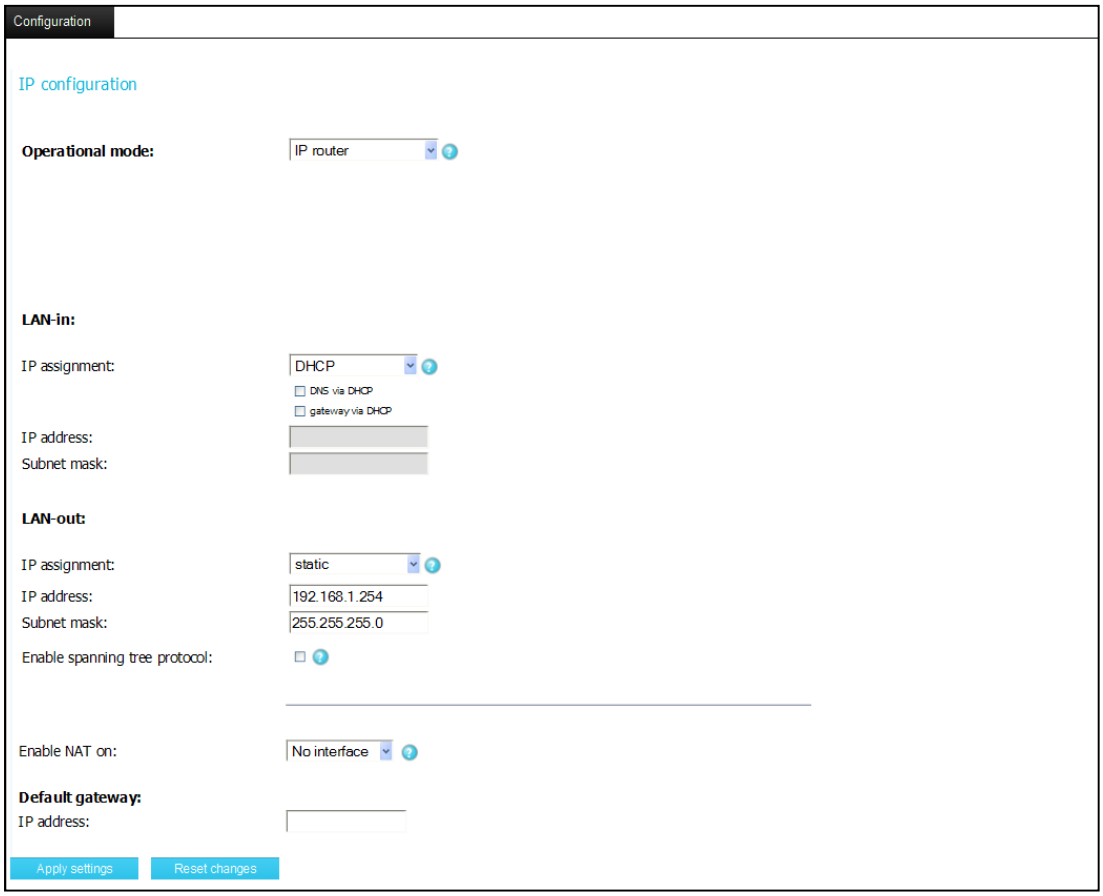
By enabling the Network Address Translation (NAT) option on the selected interface, a private IP address range is masked with a global IP address. Activating NAT is recommended with DSL/PPPoE connections.

Standard gateway:

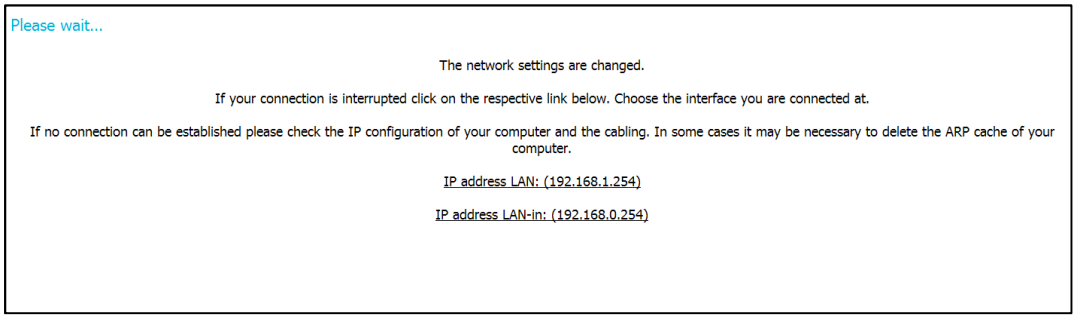
In this option, you can specify the IP address of the used gateway.

EXAMPLE

The following example shows, how to change the IP-adress from 192.168.0.254 to 192.168.1.254.



Click subsequently on: **Apply settings**


Please wait...
The network settings are changed.
If your connection is interrupted click on the respective link below. Choose the interface you are connected at.
If no connection can be established please check the IP configuration of your computer and the cabling. In some cases it may be necessary to delete the ARP cache of your computer.
IP address LAN: (192.168.1.254)
IP address LAN-in: (192.168.0.254)

Now your changes are activated.

Warning:

If the IP router mode is selected, the IP address of the LAN-in port is switched to the IP address of the LAN-out port. Now, a new IP address must be defined for LAN-in. If you configure your firewall from LAN-in to LAN-out you might have no longer access to the web interface under certain circumstances. In order to get back to the web interface, the IP address of your PC must be adapted and the previously defined IP address for LAN-in must be entered in the address line of your web browser.

After changing the IP-adress, you have to open your web browser enter the new IP-adress to get to the webinterface of the device.



© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

(IP ROUTER (EXTENDED)

If IP router (extended) is selected, the four ports of the LAN-out switch will be separated in four individual LAN-out ports. By separating the four IP interfaces you can, for example, operate several subnets.

If a special OpenVPN-Setting is chosen, the LAN-out (internal) interface is available. It is exclusively used for Open VPN channels. If this mode is selected, you will obtain specific setting opportunities for each LAN-out port on the respective page (DHCP, prioritisation, IP routing...).



Note:

802.1q VLAN Tagging cannot be used in this operating mode. (function is disabled)



Note:

Since this mode is controlled by the software, the full bandwidth of 100Mbits per second is not available between the LAN-out ports.

LAN-in Switch:

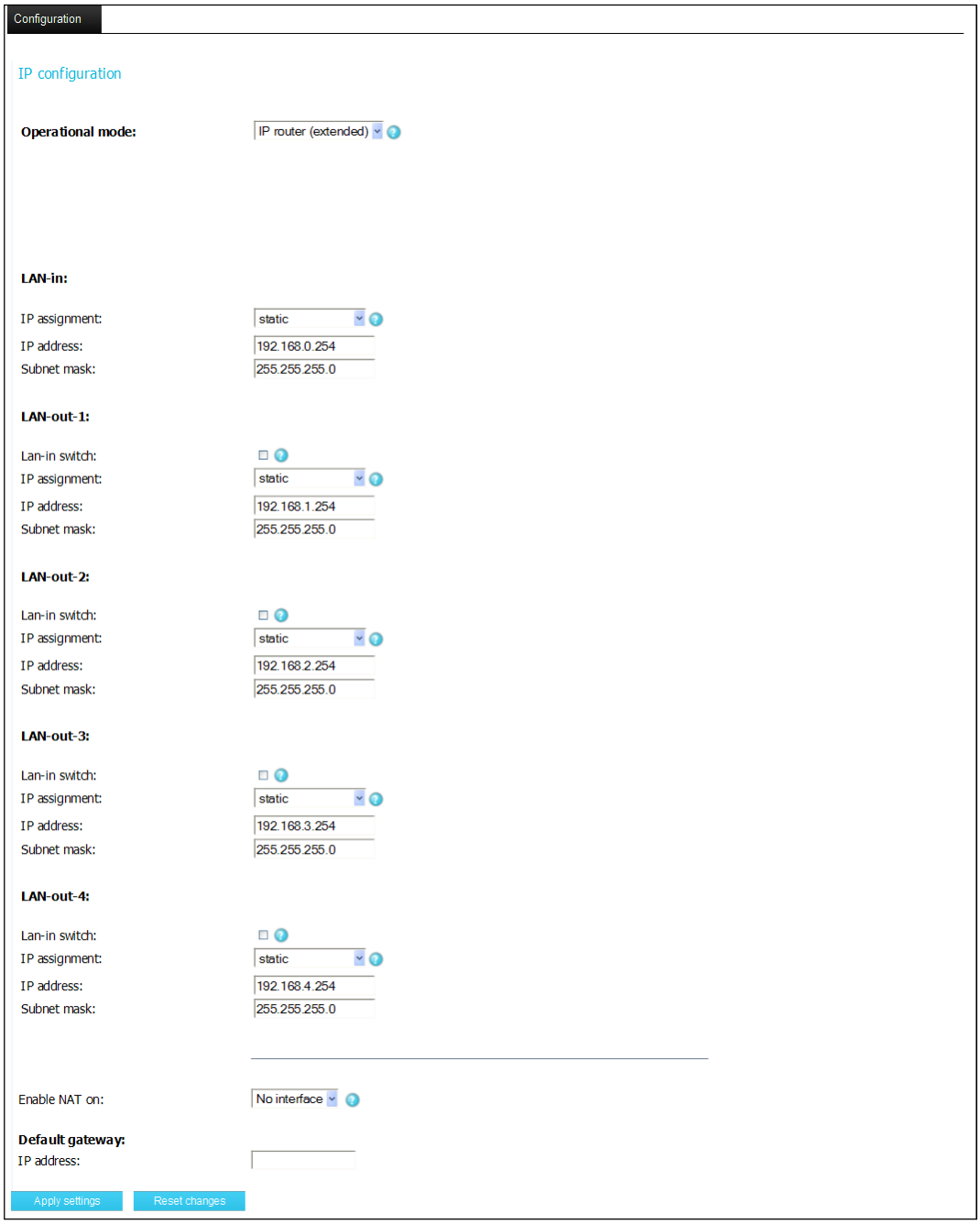
If this function is enabled, the respective LAN-out port is bridged to the LAN-in interface. The respective port acts like a switch, which is connected to LAN.in. Notwithstanding this rule, NAT settings are applied to the continuous traffic. The IP-adress of this port is the IP-adress of LAN-in.

Activate NAT on:

By enabling the Network Address Translation (NAT) option on the selected interface, a private IP address range is masked with a global IP address. Activating NAT is recommended with DSL/PPPoE connections.

Standard gateway:

In this option, you can specify the IP address of the used gateway.



© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

8.3.2 SECURENOW!

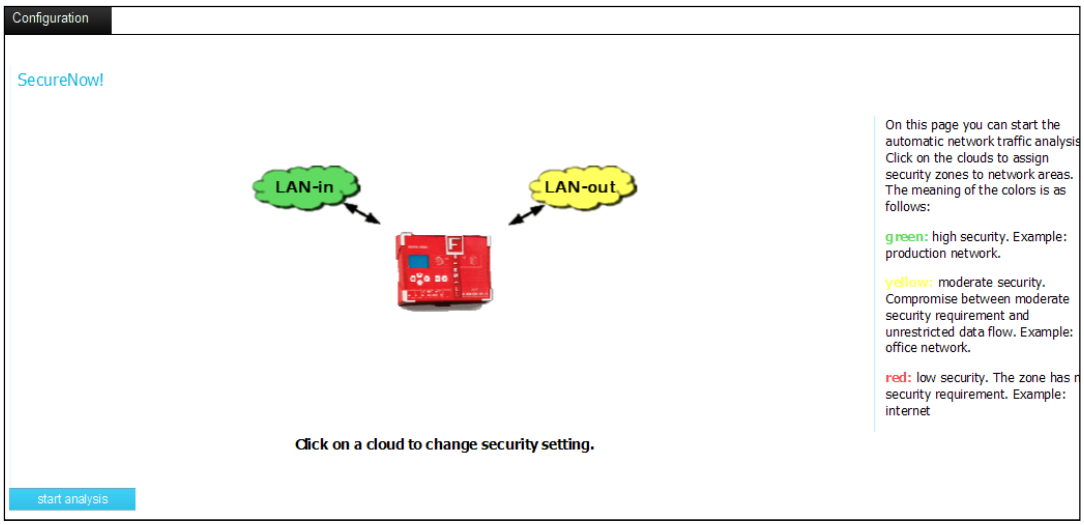
GENERAL INFO

SecureNow! allows everybody the achievement of a maximum security for local networks with only very little interaction. In order to ensure this, SecureNow! is analysing the network traffic passing through the industrial firewall and is generating precisely tailored filer rules for ebtables (in Transbridge mode) or iptables (in IPRouter or IPRouter5Port mode) based on this information.

START PAGE

At the start, the user defines for all enabled interfaces of the IF1000 series device individually, which security requirements apply. Three security levels are available for selection: High, medium and low. SecureNow! is going to generate particularly strict rules for a zone with high security level. With the medium security level, the rules are less strict in order to meet requirements like they would be present in office networks, for instance. The low security level should be used for the uplink, e.g. for the interface connected with the Internet. This zone's rules are strict with respect to the traffic coming from it, on one hand. But the traffic directed from the higher security level to the lower one is - if in doubt - always permitted. This, as a result, is always valid for the lowest level.

The network traffic recognised as critical for security is an exception. In order to recognise it, SecureNow! has a database, in which frequently used protocols are evaluated with respect to their security.


Configuration
SecureNow!
LAN-in
LAN-out
On this page you can start the automatic network traffic analysis Click on the clouds to assign security zones to network areas. The meaning of the colors is as follows:
green: high security. Example: production network.
yellow: moderate security. Compromise between moderate security requirement and unrestricted data flow. Example: office network.
red: low security. The zone has n security requirement. Example: internet
Click on a cloud to change security setting.
start analysis

The user can switch to the next security level by simply clicking with the mouse on one of the clouds. On the right hand side, you'll find a note explaining the significance of the zones by means of examples.

CAPTURE MODE

In IP-Router Mode it is neccessary to select the network layer (Layer 2 / Layer 3) which should be analysed, before executing thje Analysis of the data packages.

Note:

If two networks are identified with the same colour (e.g. yellow), the rules for the traffic between these zones will allow all packets.

8.3.4 PACKET FILTER

The packetfilter supports you in creating firewall rules in such way that a step-by-step user interface creates prompts for the most frequently used configuration parameters of firewall rules.


Layer 2
Layer 3
Status
Layer 2 Filter
2 rulesets
1 ARP* (1 rule)
ARP address resolution
2 Allow_L2* (1 rule)
Allow all L2 traffic
Add a new ruleset
By using the plus symbol you can add new rulesets
Show rulesets for following interfaces
only rules affecting the selected network interfaces will be displayed
from: * to: *
Apply settings

Note:

→The rules are processed in their respective order, starting with the first rule set.

→A certain rule set is only considered for a package if the "IN/OUT" interface setting corresponds with the package in question.

→If data is processed with a rule set, the rules included in the set are applied from the top to the bottom.

→As soon as the rule in a currently processed rule set perfectly matches the package, the corresponding action is executed and no more rules are applied.

Every rule set can contain up to 10 rules, where all rules of a rule set have the same settings with respect to the inbound and outbound interface. All active layer 2 rule sets are displayed on the main page of the package filter.

Thanks to a filter function at the bottom of the page, the displayed rule sets can be restricted by specifying the inbound and outbound interface. This has no impact on the functioning of rules: the rules not displayed are still enabled.

The toolbar for adding new rule sets is located above the filter function for the inbound and outbound interface. By clicking on the Plus icon, a dialogue window pops up, which guides the user step by step through the setup options for different protocol levels.

In IP router mode with layer 2 selected in the advanced settings, only Open VPN interfaces can be filtered. Layer 3 level allows the filtering of all interfaces in any direction, as long as they have an IP address.

Only those rule sets, for which the inbound and outbound interface as well as the direction of communication is a match, appear in this list.

Note:

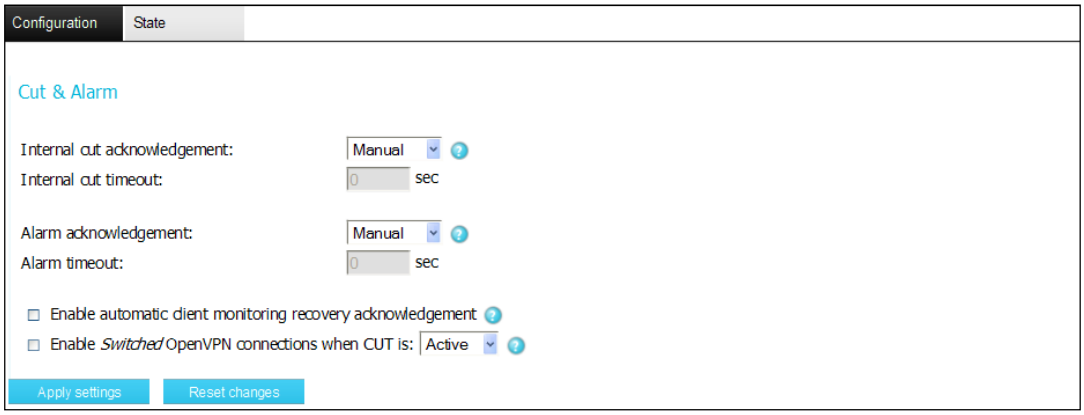
*After defining the rules, the button **Apply changes** in the web interface must be activated for testing this function.*

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

8.3.5 CUT & ALARM

CONFIGURATION

Under Cut & Alarm, you can set up how the firewall should behave in the event of a CUT (breach of the rule).



The display can be updated by using the **Apply settings** button.

The following menu items are available for selection:

Automatic acknowledgement:

The automatic acknowledgement function automatically releases the lock (CUT) after a preset period.

Manual acknowledgement:

The manual acknowledgement function does not automatically release the lock; the CUT must instead manually be confirmed or acknowledged.

Enable automatic client monitoring recovery acknowledgement

Resets the Cut & Alarm message as soon as the device is available again.

Enable Switched OpenVPN connections when CUT is

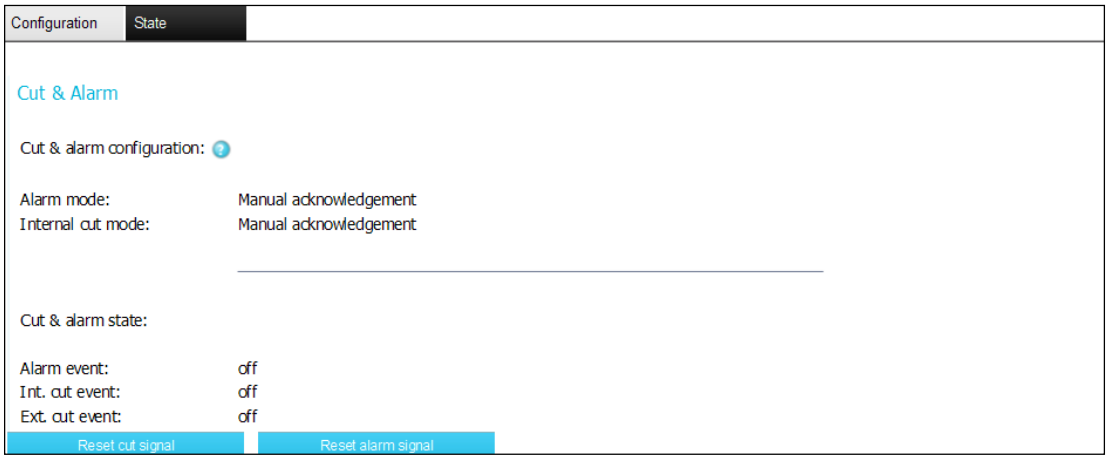
If this option is active, the OpenVPN connections will be triggered through the Cut signal. This only affects OpenVPN "switched" connections from the state to set.

Note:

This option should only be used if the Internal Cut & Alarm is set to Manual.

STATUS

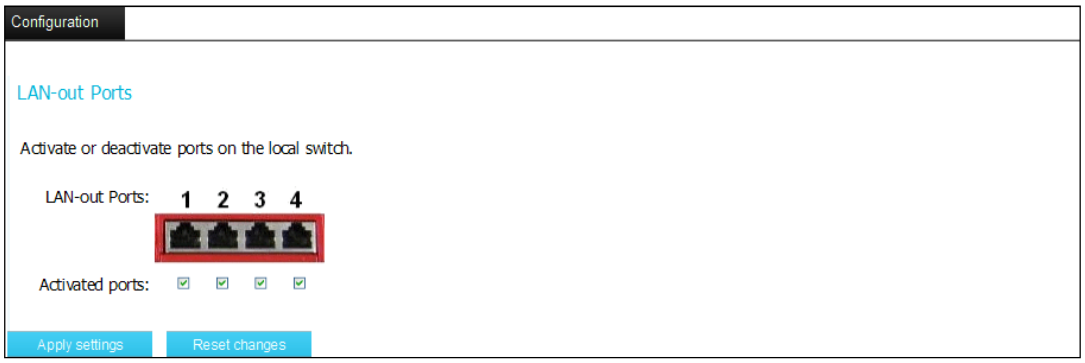
The CUT & ALARM state display shows the current Alarm mode or Internal cut mode configuration.



© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

8.3.6 LAN- OUT

All interfaces have their own setup options, which have an impact on how the interface works. Furthermore, individual ports can be activated or deactivated at the LAN-out interface for security reasons.



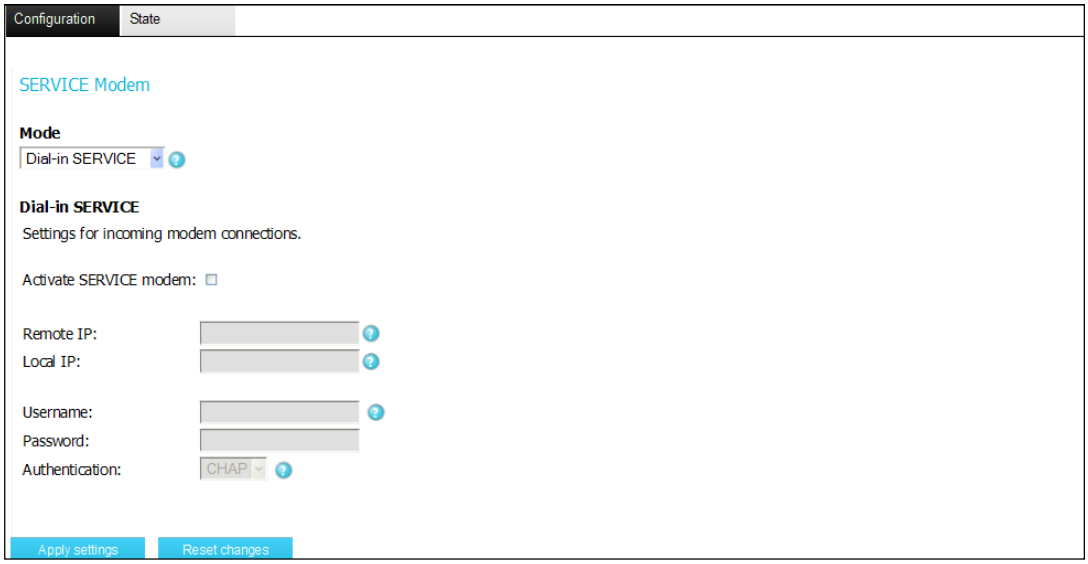
In order to deactivate a LAN port, you have to untick the box for the respective port.

Confirm this action subsequently with **Apply settings.**

8.3.7 SERVICE MODEM

CONFIGURATION

Before activating the **Service** interface you have to define in which operating mode the service interface is used. You can select between the **Dial-in service** and the **dial service** mode.

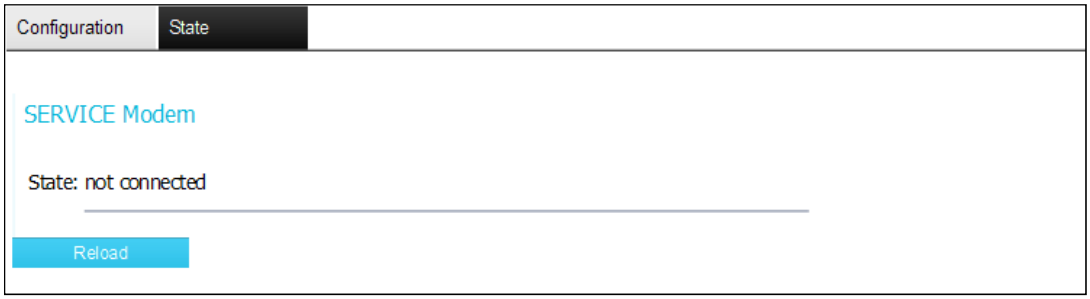


Note:

For detailled information about the service-port, see the use-case „Service".

STATE

The service menu item will show if there is a remote terminal at the service port.



© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

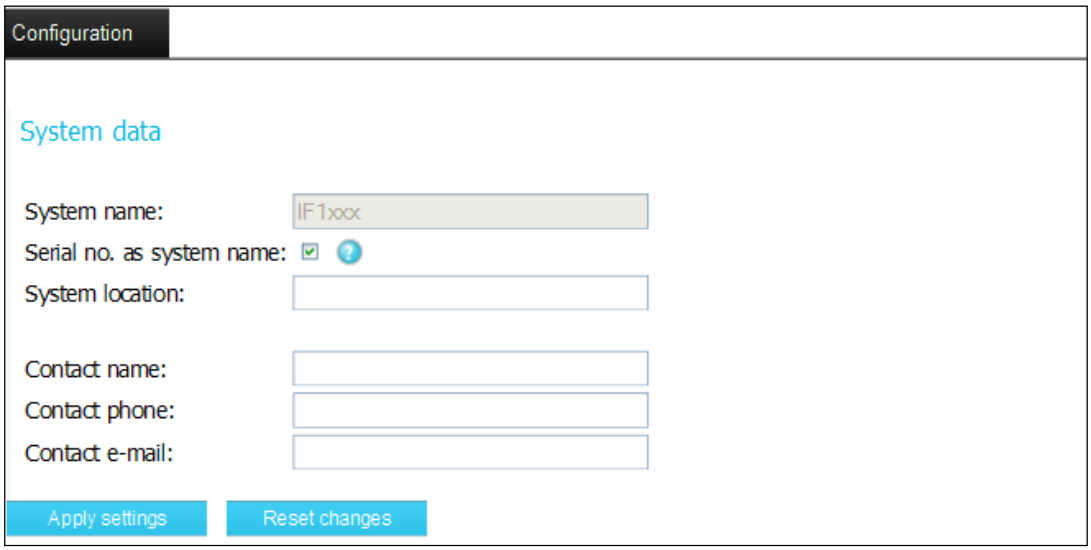
8.3.8 BASIC SETTINGS

SYSTEM DATA

In the **System data** menu, important data like the system name and the firewall location in the system, as well as the contact name of a potential service employee can be stored. This information is used for unambiguous identification of the device at its location and of the corresponding contact data, which you can view here in a service case.

Serial no. as system name:

This option is activated as default and uses the device serial number as system name.



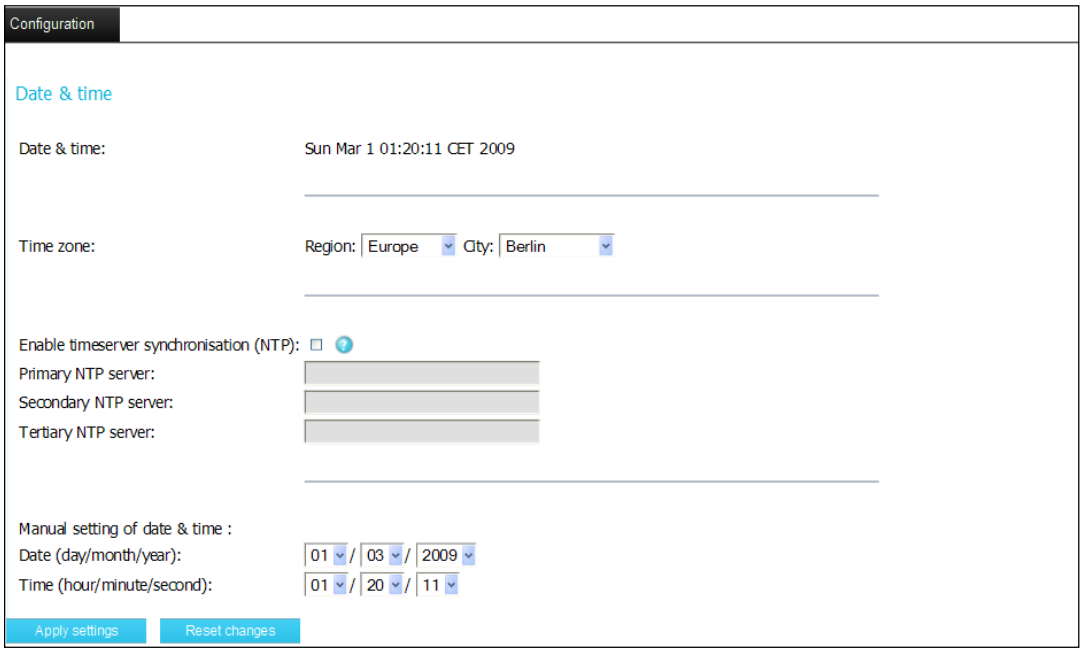
For confirming the settings you made, please click on: **Apply settings**

DATE & TIME

By using the **Date & time** menu, date and time can be configured.

The firewall does not have a real time clock. Because of that, the settings will fall back to the last saved data.

By entering and activating the IP address of the NTP server, the time setting will automatically be synchronised.



Date and time can either automatically via an NTP server or, as an alternative, be set manually.

Time zone:

The pull down menu allows the proper time zone to be set. GMT (Greenwich Meridian Time) represents the middle-European time zone, which can be adapted depending on the time shift.

Enable timeserver synchronisation (NTP):

This function allows synchronising date & time via three different NTP servers. As soon as a certain NTP server successfully responds, it will be used.

Please tick the checkbox next to this option and enter the IP-address of the NTP server.

Manual setting of date & time:

Here you can set the current date & time manually.

In order to save your changes, please click on **Apply settings.**

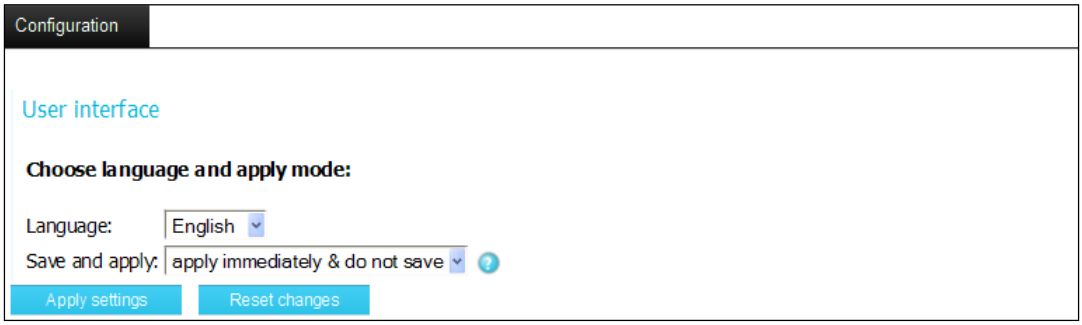
Note:

The correct setting of date and time is important for creating certificates, for evaluating event log entries, and for time based rules. Without any activated NTP server, settings will be lost after a power cut and must manually be set.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

USER INTERFACE

In the **User interface** menu, you can set language and apply mode of the web interface.



You can choose between German and English. This is set by using the pull down menu.

In the **Save & apply** pull down menu, you can choose from the options **Apply immediately & do not save** or **Save only & do not apply**.

The **Apply immediately & do not save** function shows an **Apply settings** button on all pages of the firewall interface, by means of which all changes in configuration are applied immediately. That means that changed options will have an immediate effect on the firewall functionality right after pushing the **Apply settings** button. You must save the settings by clicking on the flashing floppy-disk icon in the upper area of the web interface screen in order to permanently retain the new configuration even after a restart!

Warning:

If changes are not saved, all changes will be lost after a power drop.

The **Save only & do not apply** function shows a **Save** button on all pages of the firewall web interface. Changed settings will not be applied, but immediately saved instead.

The **Please wait** dialogue shown when transmitting a page is not applicable here. Instead of the floppy-disk icon, a restart icon, which brings you back to the start page where you can perform a restart, will flash now.

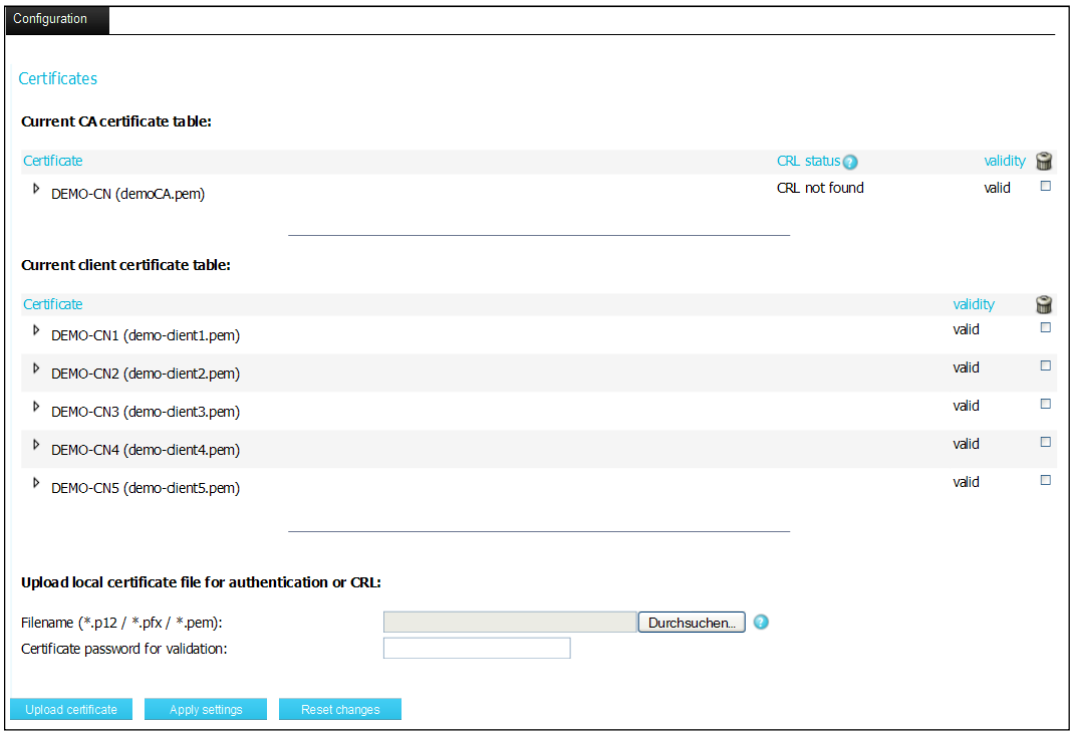
Note:

*Exceptional cases, for which the **Please wait** dialogue is displayed, are specific actions like the PING test or firmware updates.*

Confirm your settings by pushing **Apply settings**.

CERTIFICATES

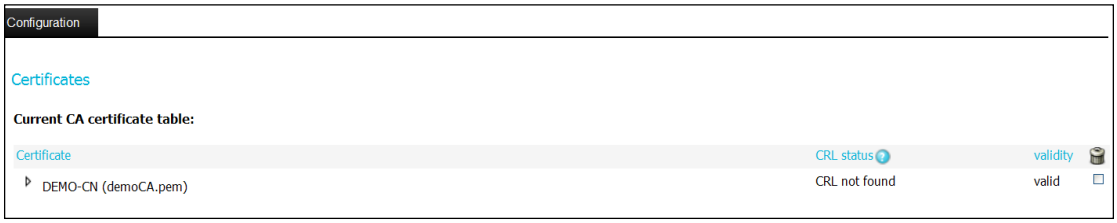
Certificates are used for authentication with L2TP/IPSec or OpenVPN connections and with the HTTPS web server in the firewall. Some demo certificates for test purposes only are already set up in this certificate administration website of the firewall.



If a certificate is uploaded its validity will automatically be verified. An invalid certificate, in which time and date settings do not match the firewall system time, will be displayed as **invalid** in the validity column. Subsequently, a question mark icon will appear for the invalid certificate, which allows retrieving further information about the system error message in English.

CRL CERTIFICATES:

The CRL status of a certificate is shown in the line below.



Individual certificates can appear to be invalid if a certificate has been withdrawn using CRL.

Note:

A client certificate file must contain both, a private key as well as a public certificate portion. The private key must be available in RSA format.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

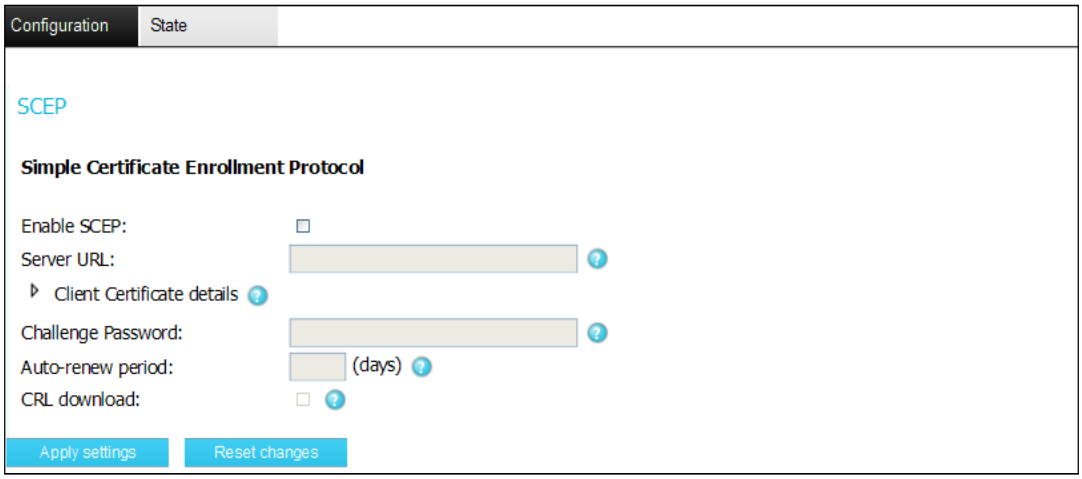
SCEP:

Allows the use of a SCEP certificate service (e.g. NDES in connection with Windows 2008 Server).

If this function is used, a certificate is automatically assigned to the device.

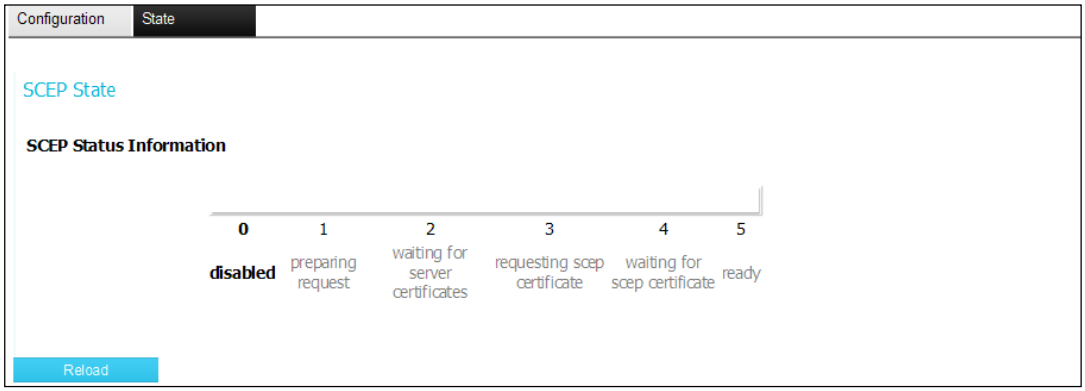
Note:

Refer to the corresponding application example for more details.



STATUS

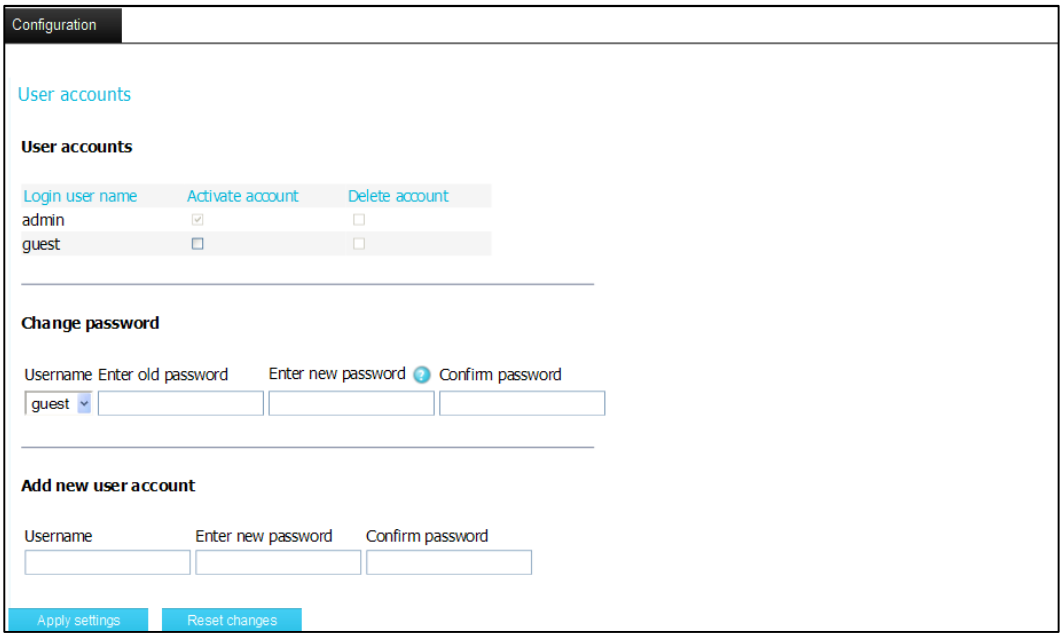
Visualises the certificate update process.



8.3.9 ACCESS CONTROL

USER ACCOUNTS

The firewall users can be created and their access rights are individually configured by using the user accounts.



User accounts

Shows the list of currently configured user accounts. Here, you can disable or entirely delete user accounts, if desired.

By enabling a guest account, a user account is created, which enables the guest user to view all device configurations, but does not allow them to make any change.

If the guest account is enabled without assigning a new password, **guest** is used as the default password. For the initial setup of a guest account password, **guest** must also be used or entered as the **old password**.

Change password

By using the **Change password** function, the password of the corresponding user account can be changed. The password you have defined here is also prompted when opening the web interface from the browser window. To change an existing password, please enter the current password in the **Enter old password** box. Select a new password, enter it and confirm it by re-entering it in the **Confirm password** box.

The **admin** user, which is previously set up and can neither be deleted nor enabled, is the only user account authorised to change the passwords of other users without having to enter the old password first.

New user account

Allows you to create a new user account. A user name and a password must be defined. Then click on **Apply settings** in order to create this account.

Note:

*The User account menu item is only used for **Account administration**. The access rights for a certain user account are assigned in the **Variable access rights** menu item.*

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

Note:

*A freshly created user account must be enabled by checking the "**Activate account**" checkbox.*

Switching between accounts:

The link **User:xxxx** at the end of the navigation bar can be used for switching accounts. Now enter the required data for the account you wish to switch. Subsequently, the new account is enabled.

Note:

*This link can also be used for logging off from the web interface. In the dialogue window, which pops up as a result, you'll have to confirm this action with **Cancel**.*



Note:

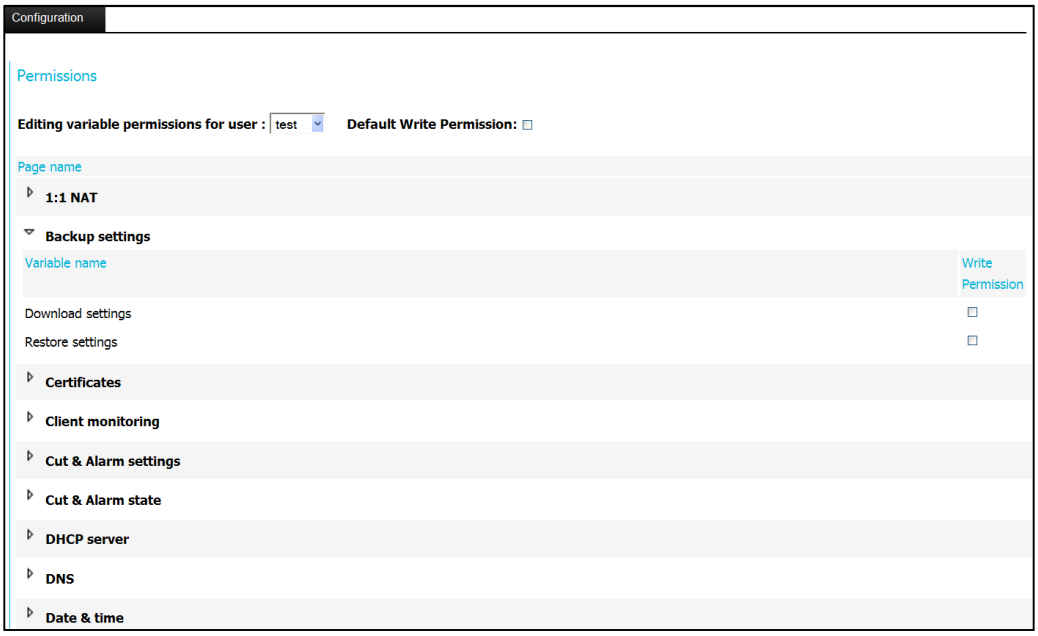
The selected password must have between 4 and 20 characters. Valid characters are: 0-9, A-Z, a-z, as well as "-._# /@".

Note:

If you have used the browser specific "Save password" option, it can happen that logging off by using the link does not work properly. Should this happen, disable this setting in your browser, if required, or select the corresponding option in your browser, which deletes any active authentications.

PERMISSIONS

By using Variable permissions, the authorisation for certain write operations, e.g. the write permission for certain areas can be assigned to a newly created user account. In the example, the **test** user account was created, which is now to be configured.



Every setting can be opened by clicking once on the corresponding setting. By checking the corresponding checkbox, you can determine for every setting, for which area the write access right should be applied.

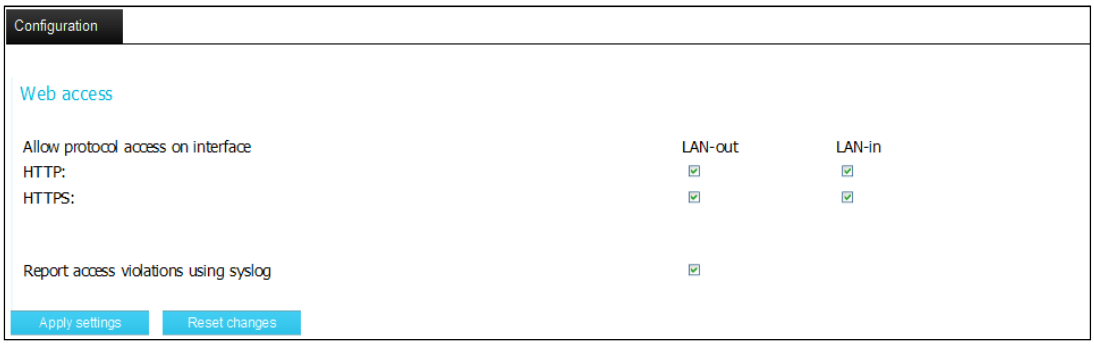
All settings made must be confirmed with the **Apply settings** button.

If you'd like to create an additional admin account, which has the same properties as the default admin account, you can check the "**Default write permission**" checkbox. But in one aspect, this account is different from the default "**admin**" account: Only the "admin" user is authorised to change the passwords of other users without having to know the old password. If you are using the "**Default write permission**", you can set up exceptions from these write permissions by removing individual write permissions by unchecking the corresponding checkbox.

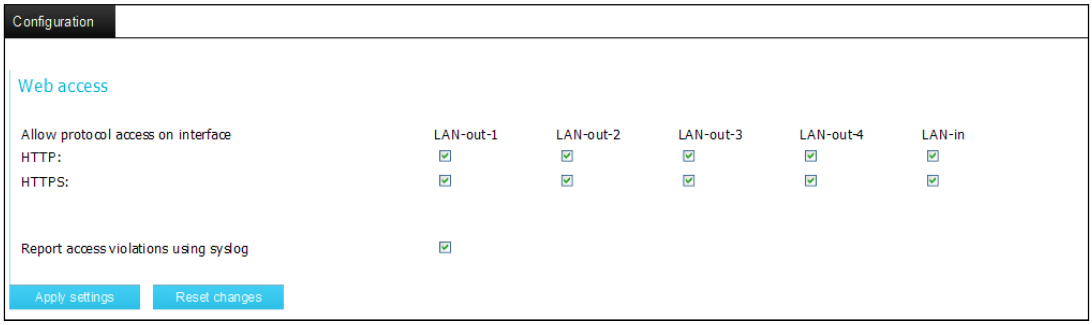
© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

WEB ACCESS

The **Webinterface access control** function depending operation mode, allows setting up access to the LAN-in and LAN-out interfaces via HTTP or HTTPS. Additionally you can set whether access violations should be reported using Eventlog.



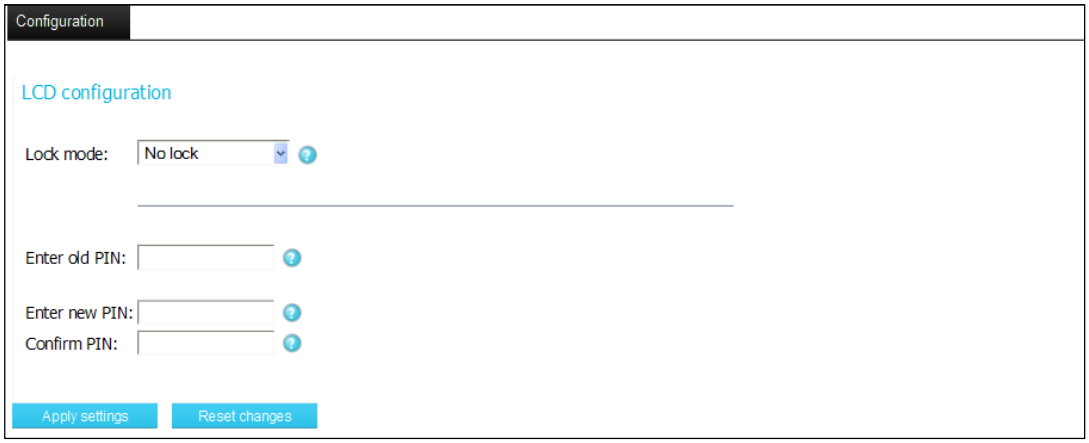
For denying a specific access type, you have to untick the checkbox next to the respective option.



Confirm your changes by pushing **Apply settings**.

LCD CONFIGURATION

The LCD configuration allows the configuration of the LC display function. The described function can also be set by using the front panel buttons on the device.

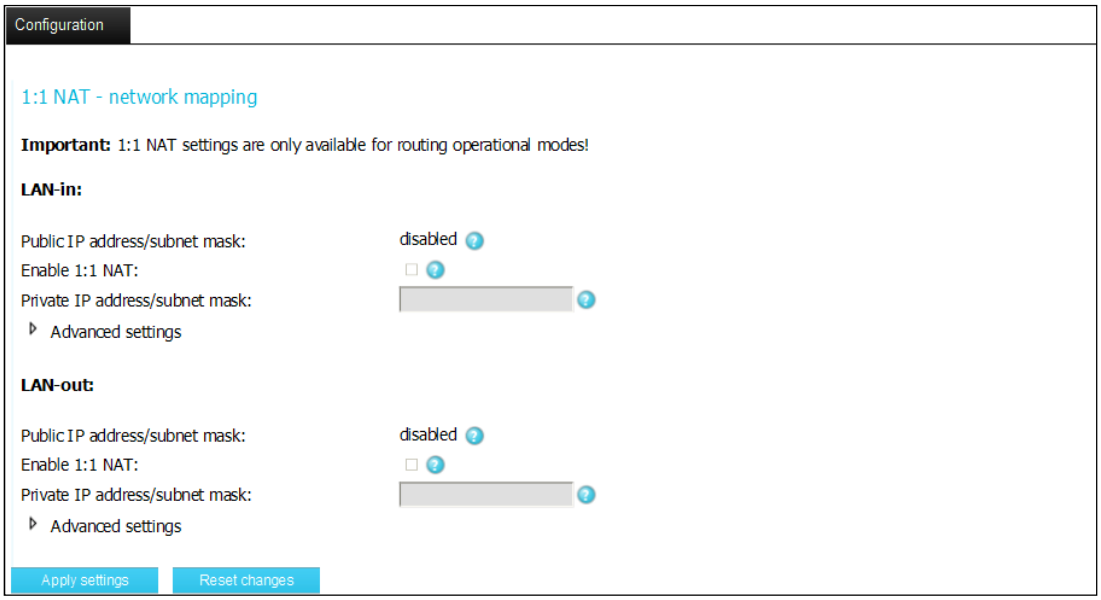


Lock mode:

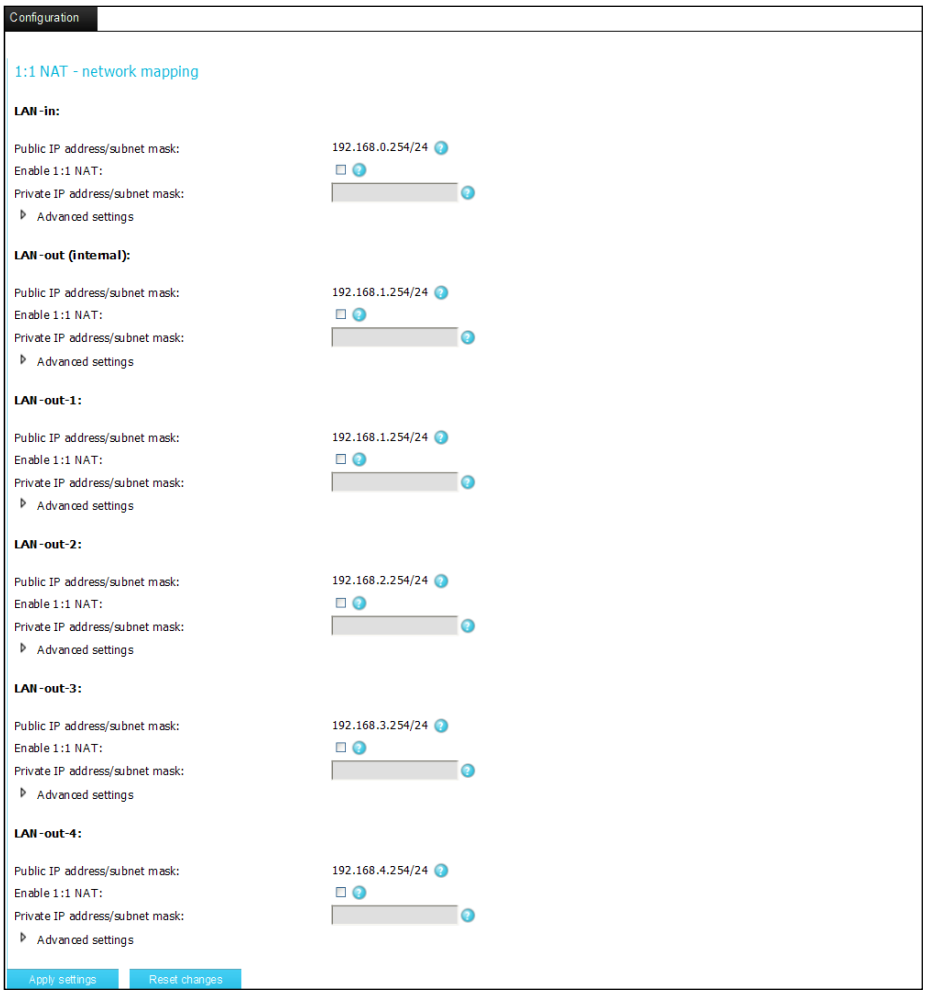
By using this function, the LCD menu and the device front buttons are locked and may be unlocked e.g. by password protection (PIN). The following options are available: No Lock, Display and Keys, or Keys only.

8.3.10 NETWORK

1:1 NAT



(Transparent bridge mode view)



(IP router mode view)

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

Activate 1:1 NAT:

Static mapping of an internal IP subnet to a subnet that can be reached externally, e.g.: If LAN-out-1 is configured with a public network address of 172.16.1.0/24, a private network with the address 192.168.0.0/24 can be entered. The result would be that a host located behind the LAN-out-1 interface with the IP address 192.168.0.1 can be reached via the LAN-in interface by using the IP address 172.16.1.1.

In the IP router (extended) mode, the same private network may be configured on all physical interfaces (LAN-Out-1 to LAN-Out-4 and LAN-In).

Private IP address subnet mask:

The private network address range must be specified in the address/subnet mask notation. So, you can e.g. enter 192.168.0.1/24. This has the effect that the firewall itself can be addressed by using 192.168.0.1 from the internal network and that, at the same time, the connected IP subnet 192.168.0.0/24 will be defined.



Note:

The 1:1 NAT option cannot be used together with the regular NAT option.



Note:

If 1:1 NAT is used in connection with IPsec, then 1:1 NAT is also applied on the IPsec connection. That means that the same global address must be defined as the local subnet address with the IPsec menu, as it is used under IP configuration.

DNS



Hostname:

The DNS host name of the device itself, will e.g. be used with Eventlog messages.

Serial number as host name::

This option is enabled by default, and allows the use of a serial number as the system name.

Domainname (Search search suffix):

The search suffix will be attached to all DNS enquiries.

DNS server:

At least one DNS server must be configured in order to transform host names into IP addresses. The device is using this in order to transform all host names, which can be specified with different parameters.

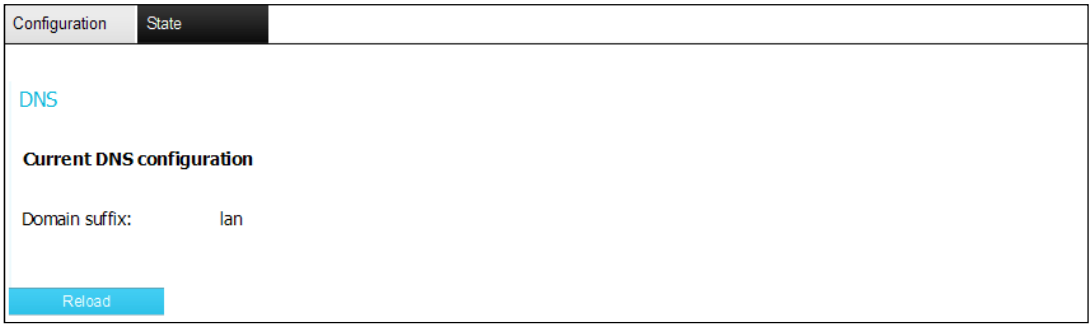
Register hostname at DHCP server:

If enabled all DHCP requests by the device will register the specified hostname at the DHCP server.

Register hostname at DHCP server:

If activated, the hostname will be transmitted at each DHCP-Request to the DHCP Server.

State:



I

Note:

If dynamical DNS Updates according to RFC2136 are supported by the DHCP server, this will lead to a valid DNS entry for the hostname on the DNS server.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

Note:

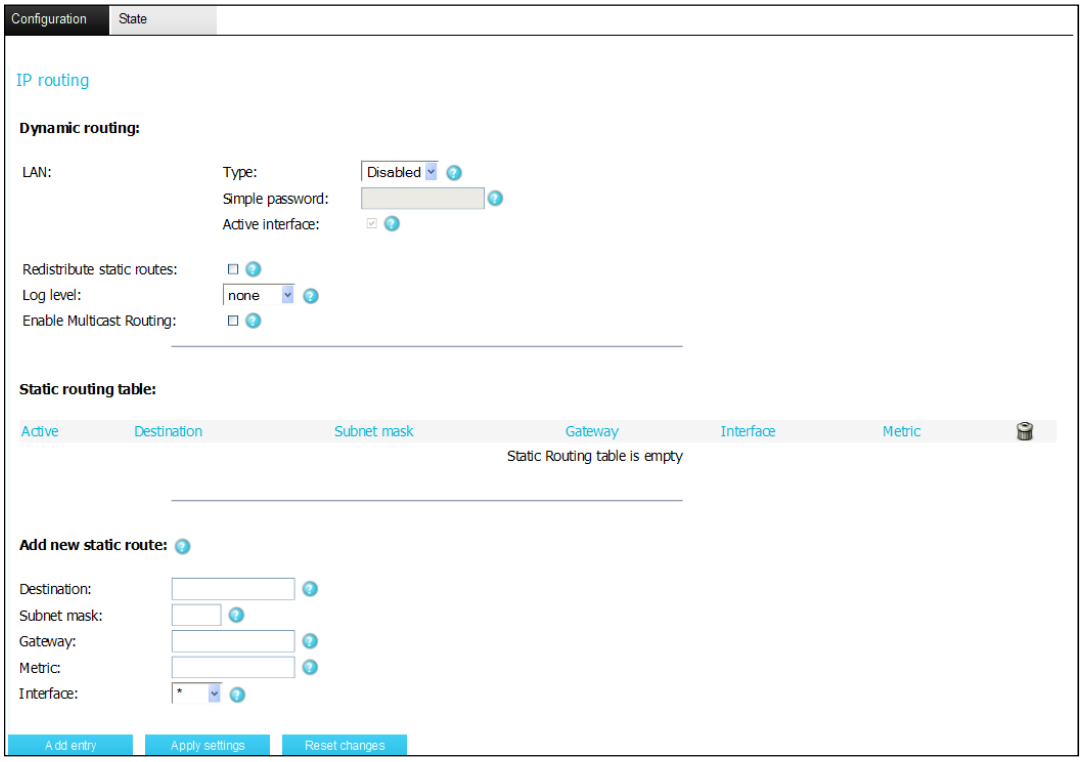
The following pages will be DNS-compatible: Date & time, Software update, SNMP Trap receiver, Open VPN Client connection-Open VPN terminal points, Ping test, Syslog server - Syslog to Email server

Note:

Manually made settings will be dynamically overwritten if an interface is configured with DHCP or PPPoE.

DYNAMIC IP ROUTING

There are two opportunities for IP routing, dynamic routing including standard routing protocols and creating a static routing table.



A static route forwards IP packets belonging to a certain network to a gateway computer (for further processing by this gateway computer). A network is defined by an IP address and by a subnet mask, which indicates how many bits starting from the left are fixed.

For instance, all addresses compliant with the form 192.168.5.x (3 bytes = 3*8 bits = 24 bits) belong to the network with IP address 192.168.5.0 and subnet mask 24. Another example is 192.168.0.0/16. All addresses complying with 192.168.x.x (2 bytes = 2*8 bits = 16 bits) belong to this network.

Due to the relationship between destination address and subnet mask, route destinations cannot be more precisely defined than the corresponding subnet mask. In other words, in the destination address, no bit be may be defined to be **1** if the corresponding bit in the subnet mask is a **0**.

The gateway specifies the forwarding IP-address or the next section IP address, by which the address set defined by network destination address and subnet mask can be reached. In case of locally linked subnet routes, the gateway address corresponds to that IP address that was assigned to the interface, which is linked to the subnet. In case of remote routes available via one or several routers, the gateway address corresponds to an IP address assigned to a neighbouring router, which can directly be reached.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen



Note:

All interfaces can be configured by using the Type, Password and Enabled Interface functions. By using the Log level menu, you can define, whether status and error messages are to be output - and if so - how often.

The following protocols are available with dynamic routing for the selected interface:

Type

RIP Routing Information Protocol:
RIP and OSPF are used and intended for dynamic creation of routing tables. RIP works with disctance vector method

OSPF:
intends circle free routing and uses the Shortest Path First Algorithmus.

Both:
Both protocols are simultaneously used with this option

Password

The Password box is optional. All routing packets are authenticated if a password is entered via OSPF/RIP. Wrongly configured routers are excluded from the network via the password function.



Note:

The password is sent as a plain text!

Enabled interface

RIP:

Router advertisements are sent on this interface if the checkbox is ticked (enabled). If you leave the checkbox empty (disabled), only arriving router advertisements are accepted, and if router advertisements are present, the interface is added to other enabled interfaces.

OSPF:

With the checkbox disabled, the interface is only added on other enabled interfaces, if router advertisements are present. In difference to RIP, inbound router advertisements are not considered.

Log level

None:

No dynamic routing messages are logged in the Eventlog.

Info:

Only a small number of status messages and critical errors are displayed.

Debug:

Comprehensive status messages, as well as error messages are displayed.

Verbose:

Detailed status and error messages, as well as information about all sent and received packets of the dynamic routing process is logged.

ADD NEW STATIC IP ROUTE

By using the IP route, IP packets can be forwarded to a specific gateway computer.

Destination network:

Here, you'd have to enter the destination network in form of an IP address

Network mask:

Enter the network mask of the destination network

Gateway:

Enter the gateway of the destination network here.

Metric:

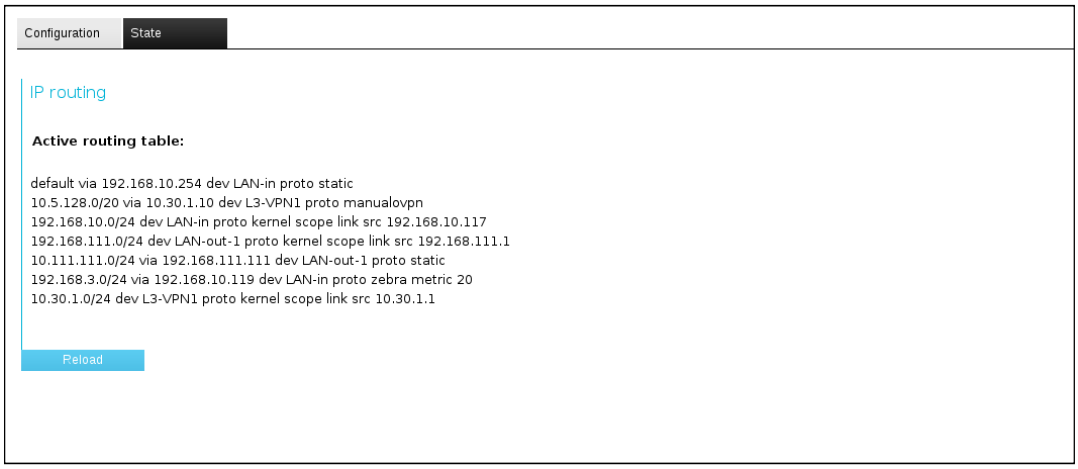
The metric defines a numeric measuring unit for the costs of a certain connection inside the network range. The Metric box is used in connection with dynamic IP routing. The admissible values are 0-100.

Interface:

Network interface for this entry.

STATUS

The Status page shows all currently enabled IP routes.


Configuration
State
IP routing
Active routing table:
default via 192.168.10.254 dev LAN-in proto static
10.5.128.0/20 via 10.30.1.10 dev L3-VPN1 proto manualovpn
192.168.10.0/24 dev LAN-in proto kernel scope link src 192.168.10.117
192.168.111.0/24 dev LAN-out-1 proto kernel scope link src 192.168.111.1
10.111.111.0/24 via 192.168.111.111 dev LAN-out-1 proto static
192.168.3.0/24 via 192.168.10.119 dev LAN-in proto zebra metric 20
10.30.1.0/24 dev L3-VPN1 proto kernel scope link src 10.30.1.1
Reload

The following routes are displayed in this example:

Line 1: Default gateway

Line 2: Routes created by the interfaces belonging to the device

Line 3: Added static route

Line 4: Routes created by the interfaces belonging to the device

Line 5: Added dynamic route

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

PORT FORWARDING

By using the **Port forwarding** menu item, it is possible to forward or initiate connections by using freely selectable ports connected to computers/addresses within the same network.



If port forwarding is to be created, it must be clear what the purpose of the forwarding is. The private port and the private IP address must be used for a local network (intranet). If no routing is to be used but a private network instead, the Private IP address box is used.

If you wish to initiate port forwarding to locations outside the local network, the public port should be used.

Note:

Refer to the corresponding application example for more details.

Note:

By using the Public IP address box, a 1:1 NAT protocol in combination with port forwarding and regular NAT can be created.

VLAN 802.1q

Thanks to the built-in firewall mechanisms, VLAN identifiers (VLAN tags) can be used in order to set up virtual subnets and to separate data traffic. For this, every subnet is using a unique number (VLAN ID) in order to identify the Ethernet packets. A device, which belongs to the VLAN with an ID of 1, can communicate with any other device within the same VLAN, but not with a device in another VLAN with an ID of 2, 3, etc. Additionally, prioritisation with VLAN is also possible. One priority can be specified for each frame (see Prioritisation menu item). This allows e.g. forwarding of control data with higher priority while HTTP data are held back.

The firewall is using an uplink port, from which it forwards the packets exactly to another port, the destination port. A packet arriving at the destination port is output at the uplink port with the corresponding VLAN ID. By using individual VLAN IDs per port, a VLAN network is set up between the Uplink and the other port, each time.



The VLAN functionality according to 802.1q is started up by using the Enable 802.1q VLAN option.

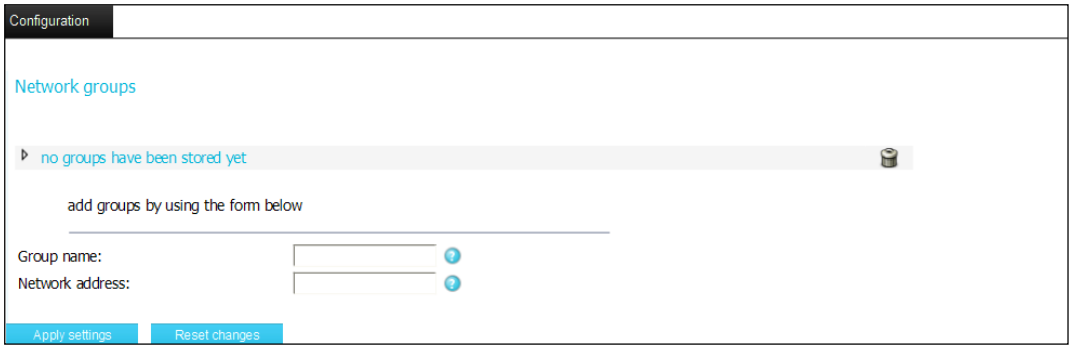
The Activate ingress filtering option discards all packets with VLAN identifiers which do not correspond to the port VLAN ID.

VLAN tags will be removed or deleted on a destination port by using the Untag on egress option. Packets without any identifier arriving at the destination port will be labelled with the VLAN ID of this port. As a result, a device at the destination port does not require any specific VLAN configuration.

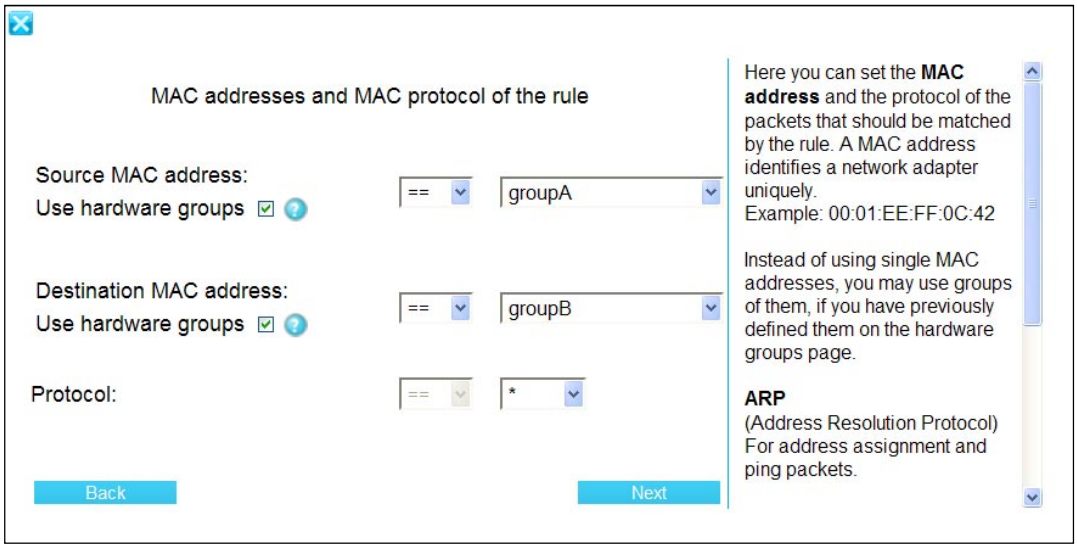
For the LAN-in interface, as well as for the four ports of the managed switch LAN-out interface, the VLAN ID can be entered in the following input boxes.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

NETWORK GROUPS



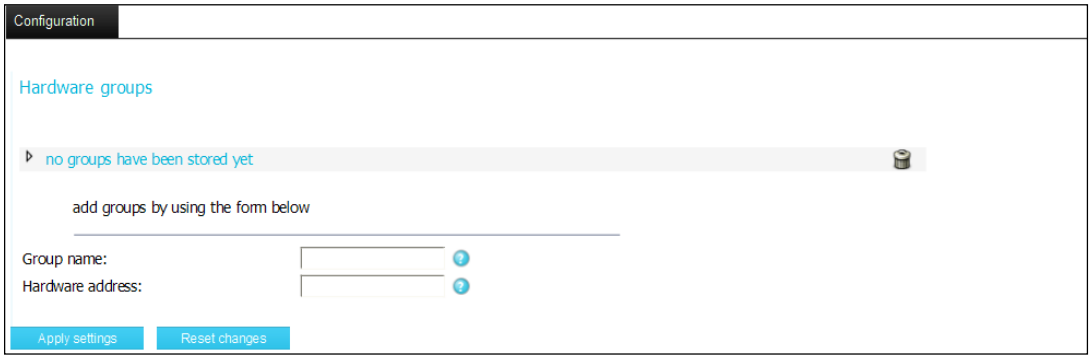
The network group function allows the grouping of IP addresses and IP subnets for use with filter rules in the Packet filter. The status line delivers information about the use of this group. The "Used in 1 rule(s)" status line information is output if a certain group is used once in the Packet filter.


MAC addresses and MAC protocol of the rule
Source MAC address:
Use hardware groups
==
groupA
Destination MAC address:
Use hardware groups
==
groupB
Protocol:
==
*
Back
Next
Here you can set the MAC address and the protocol of the packets that should be matched by the rule. A MAC address identifies a network adapter uniquely.
Example: 00:01:EE:FF:0C:42
Instead of using single MAC addresses, you may use groups of them, if you have previously defined them on the hardware groups page.
ARP
(Address Resolution Protocol)
For address assignment and ping packets.

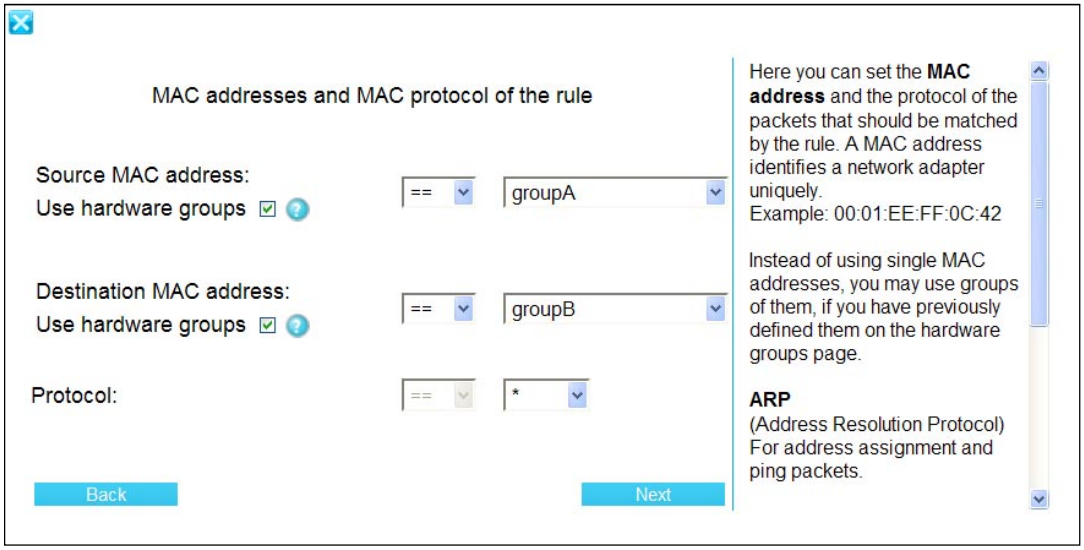
The rule as shown here would result in 2 system entries.

Note:
The use of ***!=*** *in the layer2 Packet filter for network groups is not supported.*

HARDWARE GROUPS



The hardware group function allows the grouping of MAC addresses for use with filter rules in the Packet filter. The status line delivers information about the use of this group. The "Used in 1 rule(s)" status line information is output if a certain group is used once in the Packet filter.


MAC addresses and MAC protocol of the rule
Source MAC address:
Use hardware groups
==
groupA
Destination MAC address:
Use hardware groups
==
groupB
Protocol:
==
*
Back
Next
Here you can set the MAC address and the protocol of the packets that should be matched by the rule. A MAC address identifies a network adapter uniquely.
Example: 00:01:EE:FF:0C:42
Instead of using single MAC addresses, you may use groups of them, if you have previously defined them on the hardware groups page.
ARP
(Address Resolution Protocol)
For address assignment and ping packets.

Note:

Hardware groups can only be used in layer2 rulesets, because only there, filtering for MAC addresses is possible.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

8.3.11 VPN

The VPN menu item allows establishing a Virtual Private Network connection based on an OpenVPN implementation.

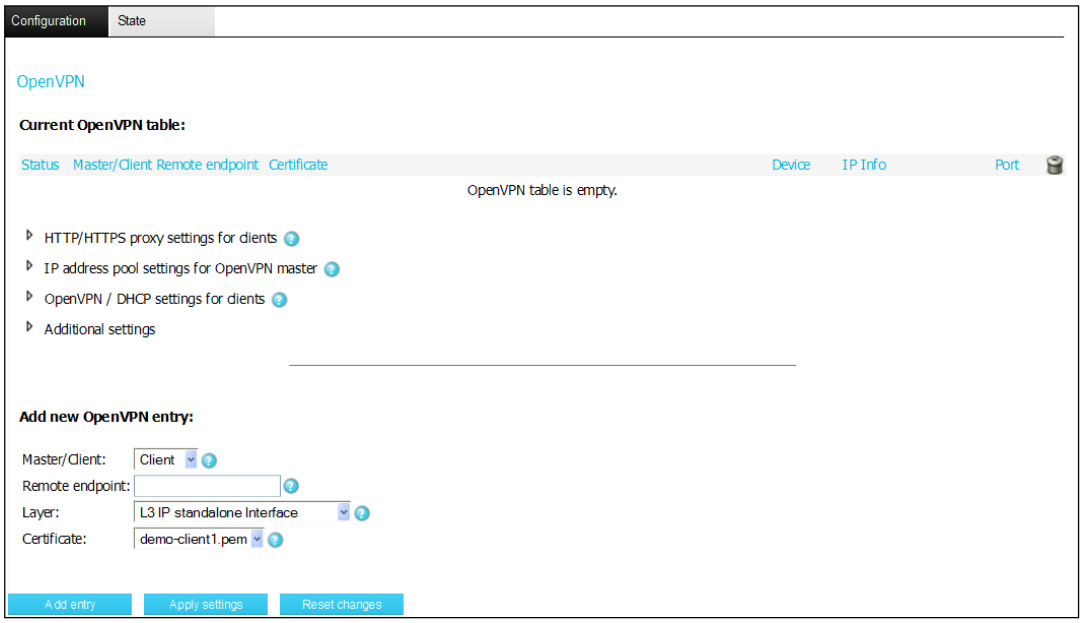
OPEN VPN

HTTP / HTTPS Proxy Settings for Clients

For Open VPN client, an HTTP proxy can be used. When using the HTTP proxy for clients, the fields must be filled out.

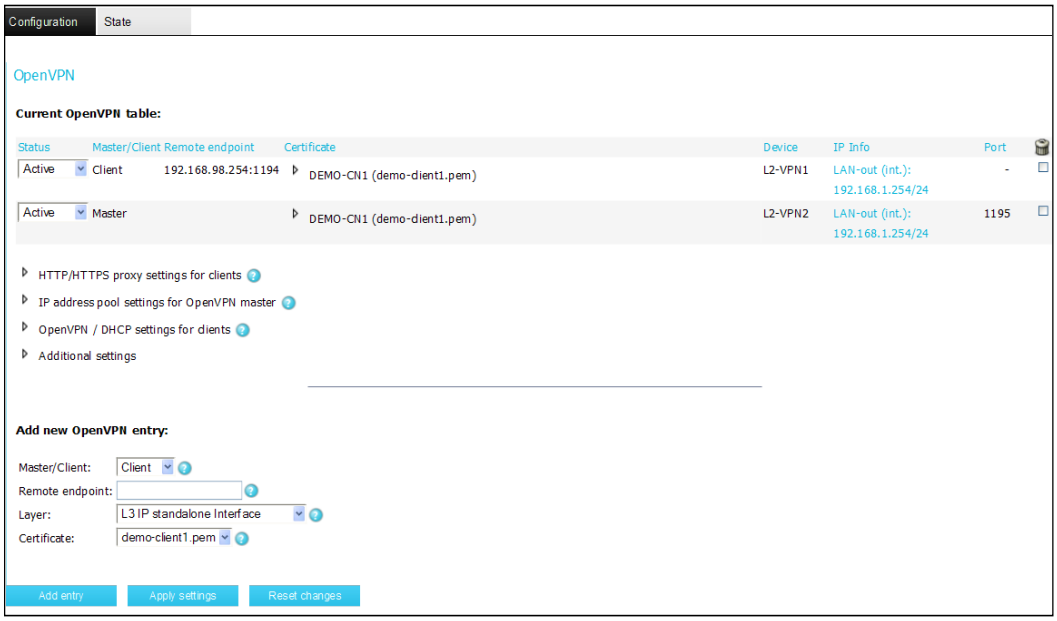
IP address pool settings for OpenVPN Server:

OpenVPN allows the automatic assignment of IP addresses to clients, similar to DHCP. Activating this option will effect that each client gets automatically assigned with an IPAddress and Subnet from the specified IP range. This option can only be used on a single Server entry. The IP address space for allocations must be within the IP subnet of LANout / LAN-out (internal) interface, to the subnet of the L3-VPN-interface in case of a Layer 3 connection, and may not already covered by the DHCP server, or some other device used. The Server Device "specifies the interface on the OpenVPN to table entry on which the IP address assignment should be used. If the drop down field is empty, a Server entry has to be created first.

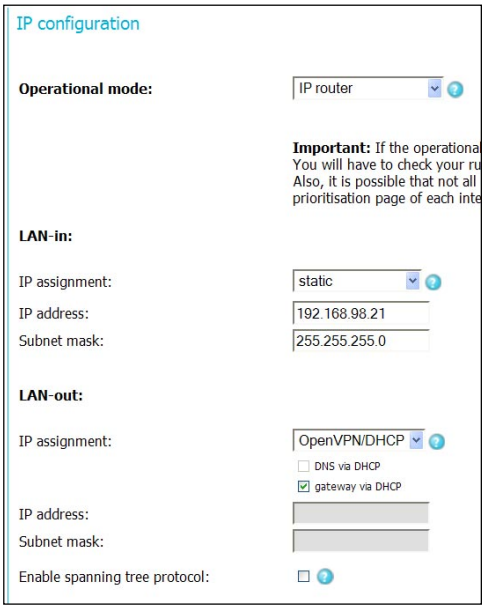


OpenVPN / DHCP settings for client

One of the OpenVPN client connections can be used to obtain the IP settings of LAN-out/LANout (internal) interface.



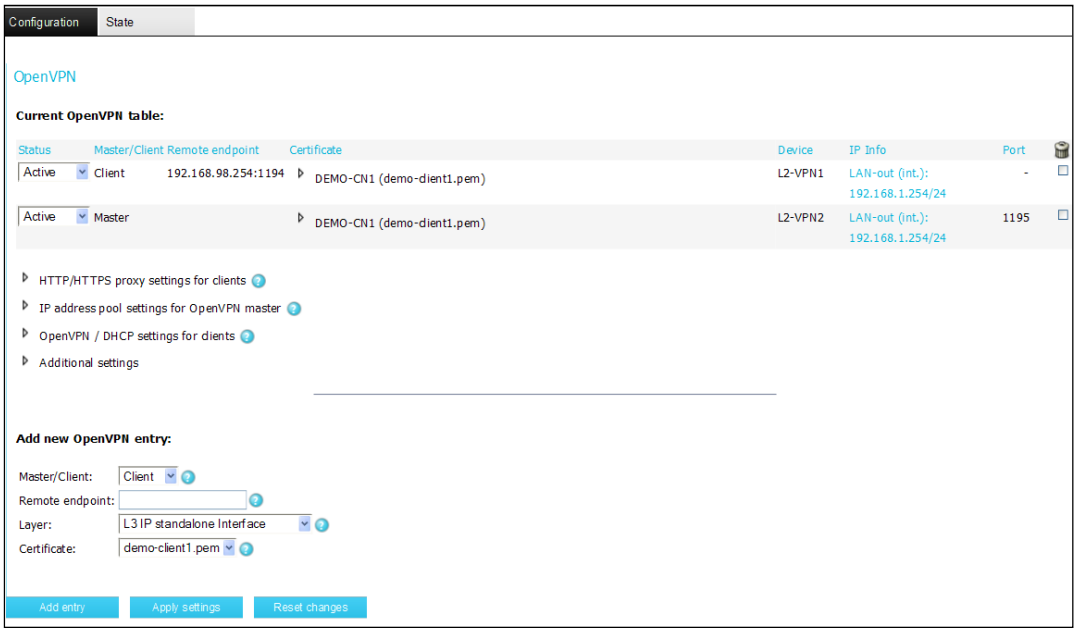
Addionally a drop down box for LANout/LAN-out (internal) for IP-assignment has to be set to OpenVPN/DHCP. The "Client-Device" sets the interface of the OpenVPN table entry, which will be used for OpenVPN. One entry is possible. If the drop down field ist empty, an client entry has to be created first. Independet ffrom Default gateway the OpenVPN Server can transfer several static routes. The checkbox will decide if they will be applied. The application of an Default Gateway which is transferred too, has to be configured on the IP-Configuration site.



© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

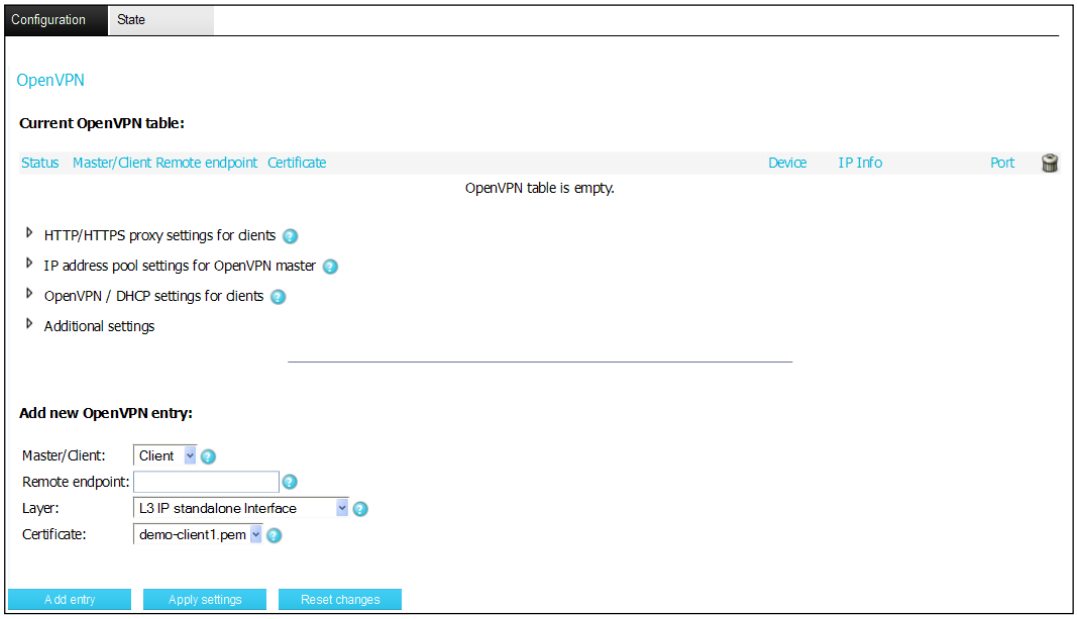
Additional Settings:

By default, the log level "info" is active. It is meant for normal operation and reports simple status information and critical errors. The log level "debug" and "verbose" is intended for troubleshooting, if a connection does not materialize and involve significant performance loss.



Add new OpenVPN entry:

The OpenVPN menu item is available for defining and configuring OpenVPN connections.



Server/Client

You have to define in the pull down menu if the firewall should work as a **Server** or **Client**. Please select the corresponding function.

In the **Server mode**, the device starts a TCP connection, on which several clients can connect. The TCP port is automatically incremented and starts with port 1194.

In the **Client mode**, a connection is established to a remote endpoint in Server mode. The endpoint must be specified in form of an IP address:Port.

Certificate:

Select the desired certificate from the pull down menu. For confirming your settings, please select **Apply settings**.

STATE

In order to display the current status, please select **OpenVPN state**, and the website will either display the states or the message "OpenVPN table is empty" if no VPN connection has been configured yet.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

L2TP

L2TP allows establishment of VPN connections from a Microsoft Windows system to the firewall. In this case, the firewall works as a server and allows up to ten client connections.



After activating this functionality by using the **Activate L2TP/IPSec server** option, the interface, over which the VPN communication should take place, must be selected. Additionally, a local IP address will be assigned to the adapter dynamically generated, in this case. This address should be in the same subnet like LAN-in and LAN-out. Authentication can now either be performed by using a PSK (preshared key) or a certificate.

Note:

If filtering using the L2TP/IPsec adapter is to be used, the user IP of the L2TP user entries must be added as a criterion in the Packet filter. A separate interface is not available, but it must be selected.*

Note:

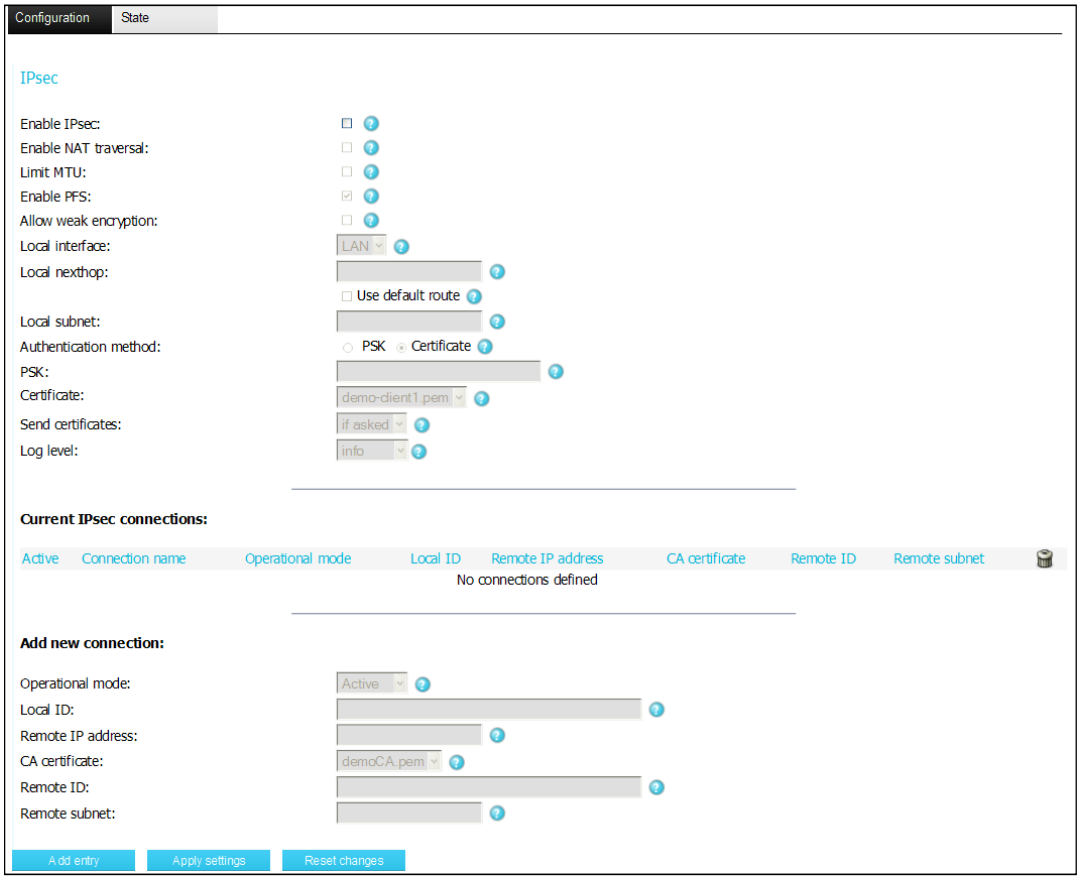
This function requires Windows XP SP2 or a later version for the remote terminal. Windows 2000 must be equipped with the corresponding Microsoft updates with respect to L2TP VPN. MacOSx is not supported.

Note:

This function is not supported if the L2TP connection is to be configured via a modem locally connected with the firewall.

IPsec

IPsec allows the encoding of the entire communication between this device and a remote endpoint on IP level. IPsec allows the encoding of subnets located behind the corresponding remote terminal.



Enable IPsec:

Enables / disables the IPsec function.

Enable NAT traversal:

This function must be enabled if the remote terminal has NAT activated.

Limit MTU:

This function requires IP packet encapsulation, which increases packet fragmentation and reduces network performance. If this is the case, it might be helpful to enable this feature but limit the size of outgoing packets.

In order to encode a connection between the firewall and a remote terminal, the following data must be specified.

Enable PFS:

With Perfect Forward Secrecy, a temporary key is generated in order to protect the data. This session key is renewed in short intervals and grants additional security.

Allow weak encryption:

If the remote terminal suggests using a non-secure algorithm (DES/DH1), it will be accepted.

Local interface:

Select the interface over which the IPsec tunnel should be created.

Local nexthop:

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

The IP address or host name of the next router can be specified here for improved availability.

Use default route:

Uses the standard gateway, which has been set up manually or via a DSL connection, as the next router.

Local subnet:

This option specifies the subnet, the traffic of which towards the remote terminal is to be encrypted. The subnet must be defined as an IP/netmask, e.g. as 192.168.0.0/24. The interface IP-address is used, if no data is entered.

AUTHENTICATION METHOD:

Authentication can now either be performed by using a PSK (preshared key) or a certificate. Certificate is the most secure connection setting.

PSK:

The generated PSK code is entered here.

Certificate:

Using this certificate, the device authenticates itself at the remote terminal.

Send certificates:

Here you can set up when certificates should be sent.

Log Level:

By default, the log level "info" is active. It is meant for normal operation and reports simple status information and critical errors. The log level "debug" and "verbose" is intended for troubleshooting, if a connection does not materialize and involve significant performance loss.

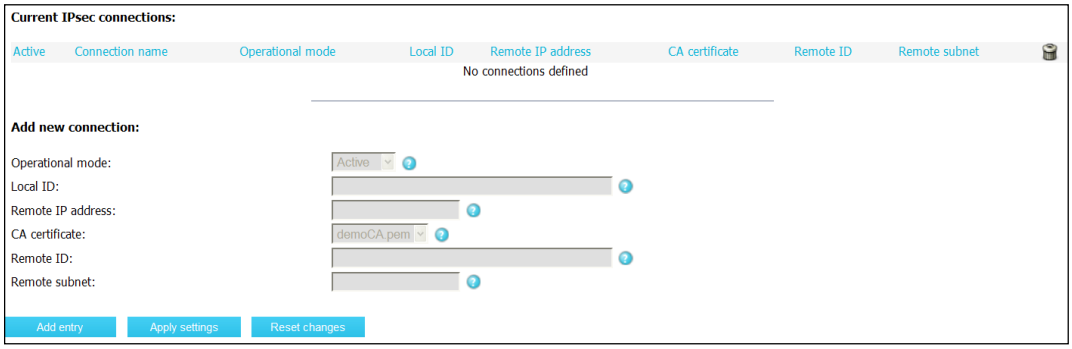


Hinweis:

Die IF1000 Firewall verwendet bei IPsec außerdem folgende Defaultparameter:

- *Dead Peer Detection Timeout: 120 Sekunden*
- *IKE Lifetime: 1h*
- *SA Lifetime: 8h*

ADD NEW CONNECTION:



OPERATIONAL MODE:

Active:

In active mode, the firewall will permanently try to establish a connection with the remote terminal.

Passive:

In passive mode, the firewall will wait until the remote terminal tries to establish a connection. This mode is required if the IP address of the remote terminal is unknown.

Local ID:

The local ID is used for identifying the remote terminal with a PSK connection. The IP address is automatically used if this box remains blank.

Remote IP address:

The IP address of the remote terminal is specified here.

CA certificate:

In order to be accepted, the certificate of the remote terminal must be signed by this CA.

Remote ID:

If the remote terminal certificates are known they can be copied and pasted here.

Remote subnet:

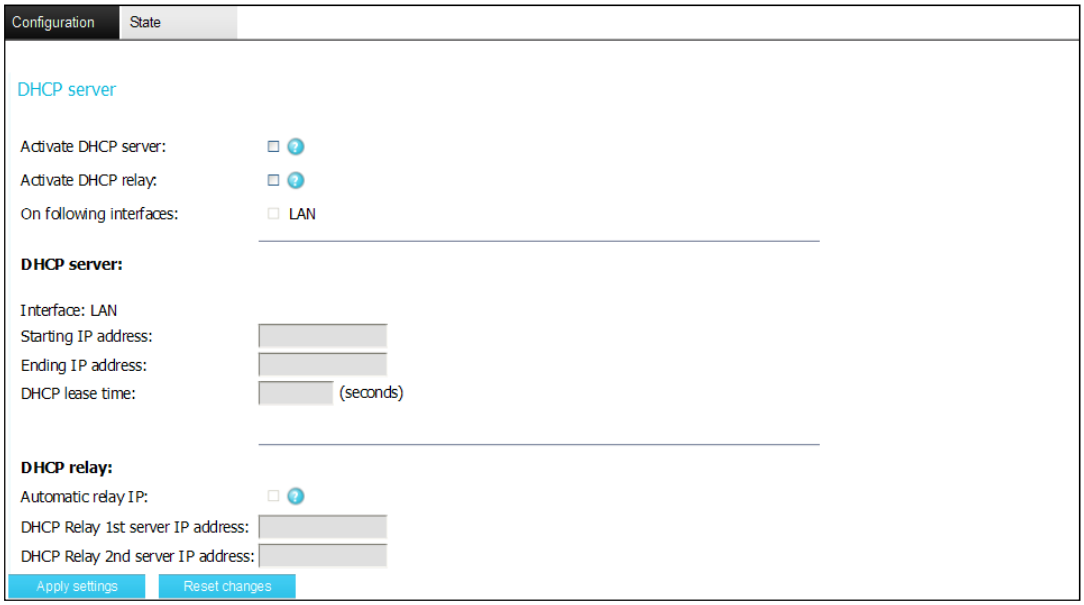
The subnet of the remote terminal is entered here. The subnet must be defined as an IP/netmask, e.g. as 192.168.0.0/24. If no data is entered the interface IP-address will be used.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

8.3.12 UTILITIES

DHCP SERVER

The built-in DHCP server can be used for distributing IP addresses. By default it is, however, turned off and may be activated by using the **Activate DHCP server** option.

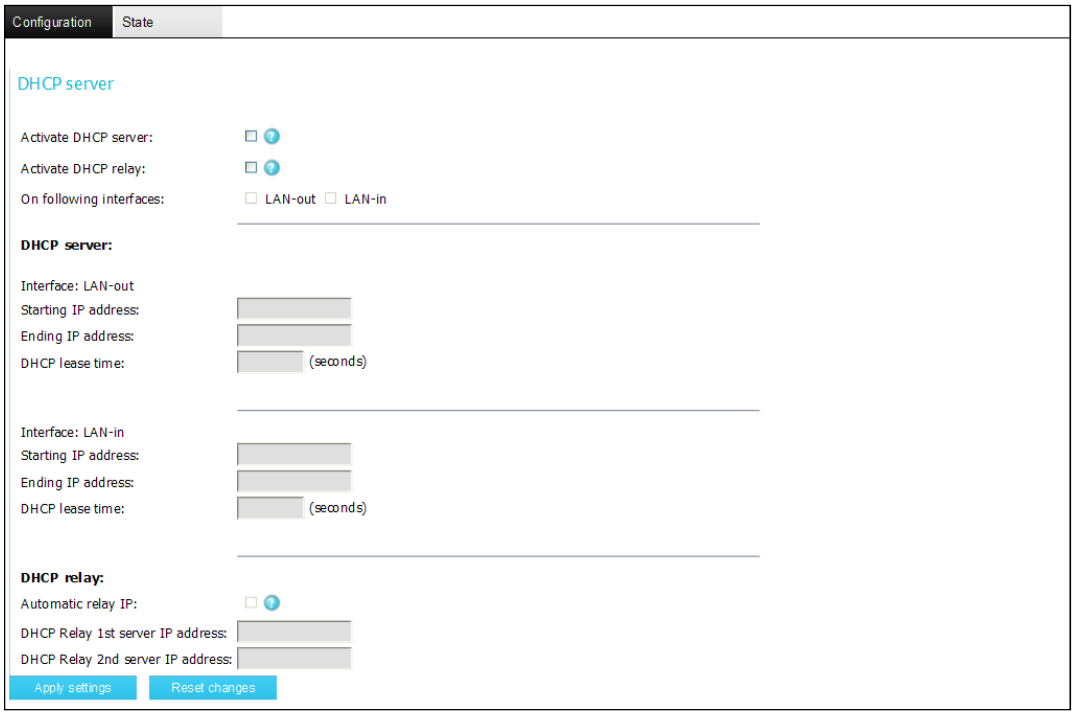


Note:

The range of IP addresses must be within the same range like the IP address of the interface used!

The interfaces, on which the DHCP server should respond to client requests can be specified in the **On following interfaces** options in more detail. The pool range can be set up separately for each interface.

Additionally to distributing IP addresses, the DHCP server can also transmit a domain search suffix and three DNS server addresses in server mode. This information is forwarded to DHCP clients. The device is using an internal DNS utility in order to buffer all enquiries. Should the firewall not work with an own static IP address but as a DHCP client, this data will be overwritten by the DHCP server used in that case.



(IP router view)

LAN-out ports may be configured individually in the IP router extended mode.

DHCP RELAY:

In the IP router mode, you have the opportunity to Enable a DHCP relay server as an alternative to the DHCP server. The DHCP relay server is used for forwarding DHCP requests via an Ethernet segment. All interfaces, on which DHCP requests are received, as well as the interface, on which the actual DHCP runs, must be selected in DHCP relay mode.

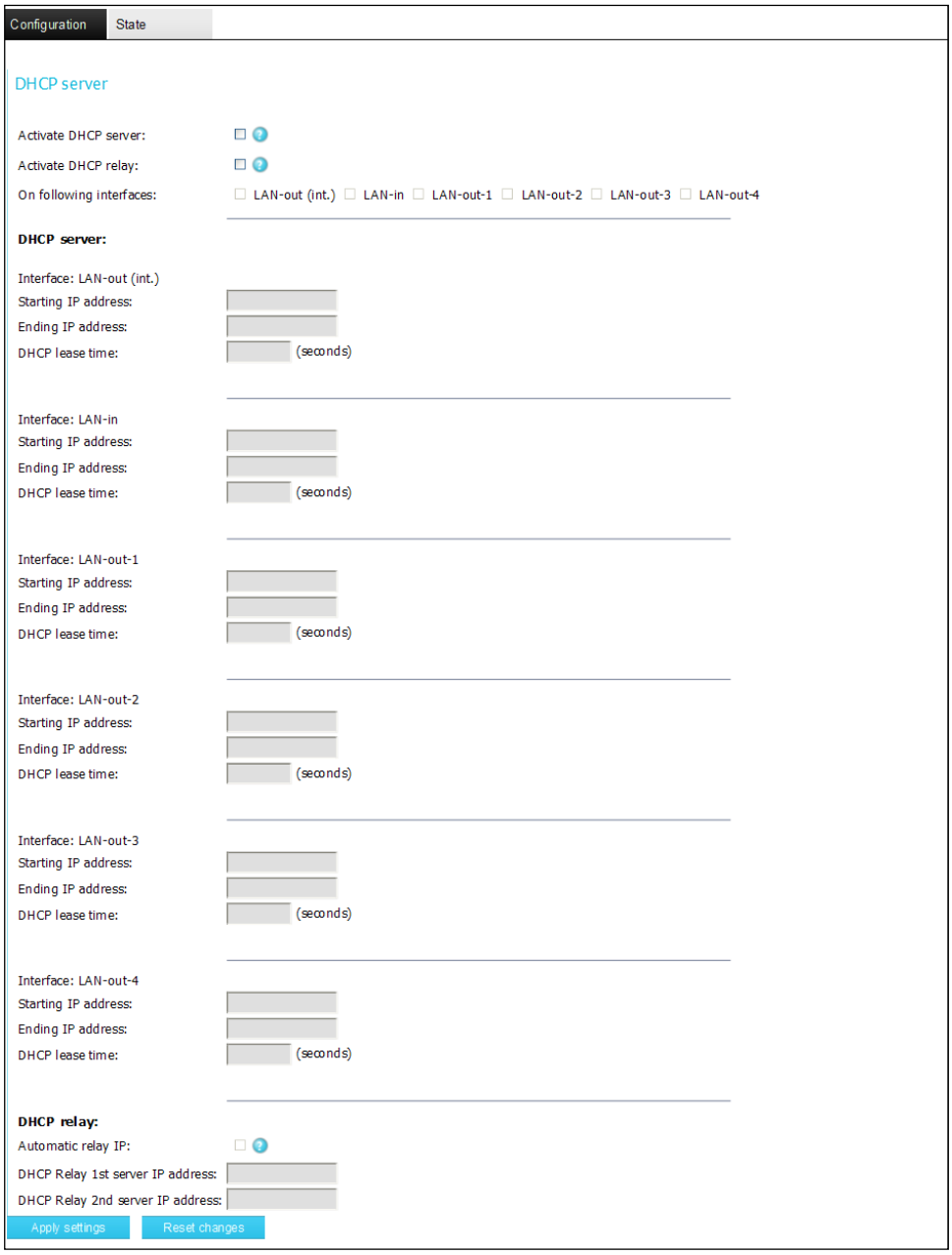
Automatic relay IP:

If this function is activated, the firewall itself works as a DHCP server and responds to requests from the selected interface.

Relay IP address:

Here you'll have to enter the IP address of the DHCP server.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

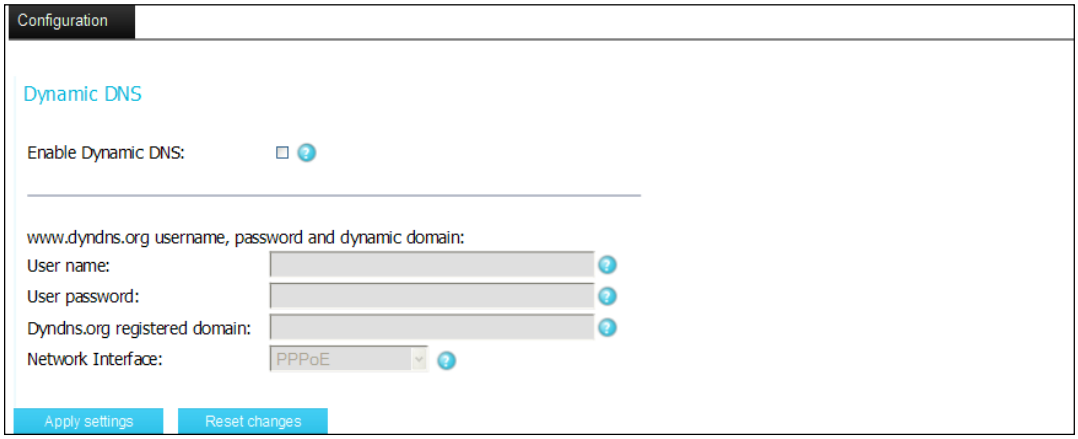


(IP router view)

LAN-out ports may be configured individually in the IP router extended mode.

DYNAMIC DNS

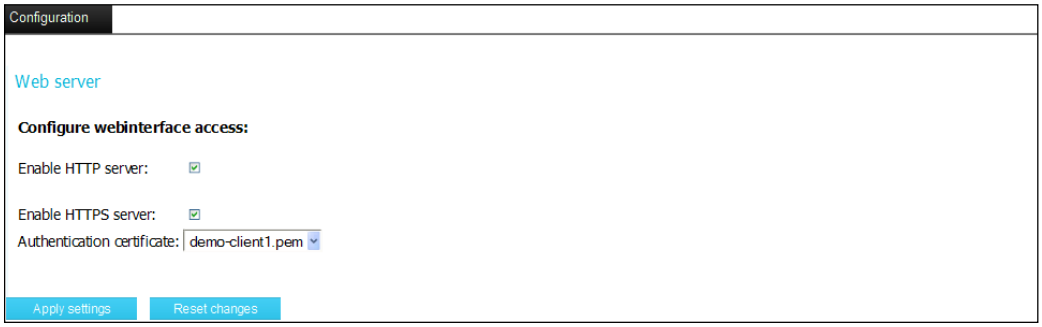
The dynamic DNS option enables communication with a remote terminal if this terminal can be accessed via the Internet. You can set up an account. on the website www.dyndns.org where can create DynDNS domains. This data consisting of User name, User password and Dyndns.org registered domain can be entered here. If this function is turned on, the firewall enables this DynDNS domain to access an IP address located behind it.



The correct Network interface must be selected in order to use this function properly. This setting depends on how the firewall is connected with the Internet. If, for instance, an analog modem is used, this is usually connected to the service port, and as a result you would have to select Service modem. PPPoE should be used if the firewall is connected to the Internet using a conventional LAN connection.

WEB SERVER

Access to the firewall web interface using the protocols http or https can be set up in the Web server > Access control menu.



The web server integrated in the firewall for configuration can only be reached using the activated protocols.

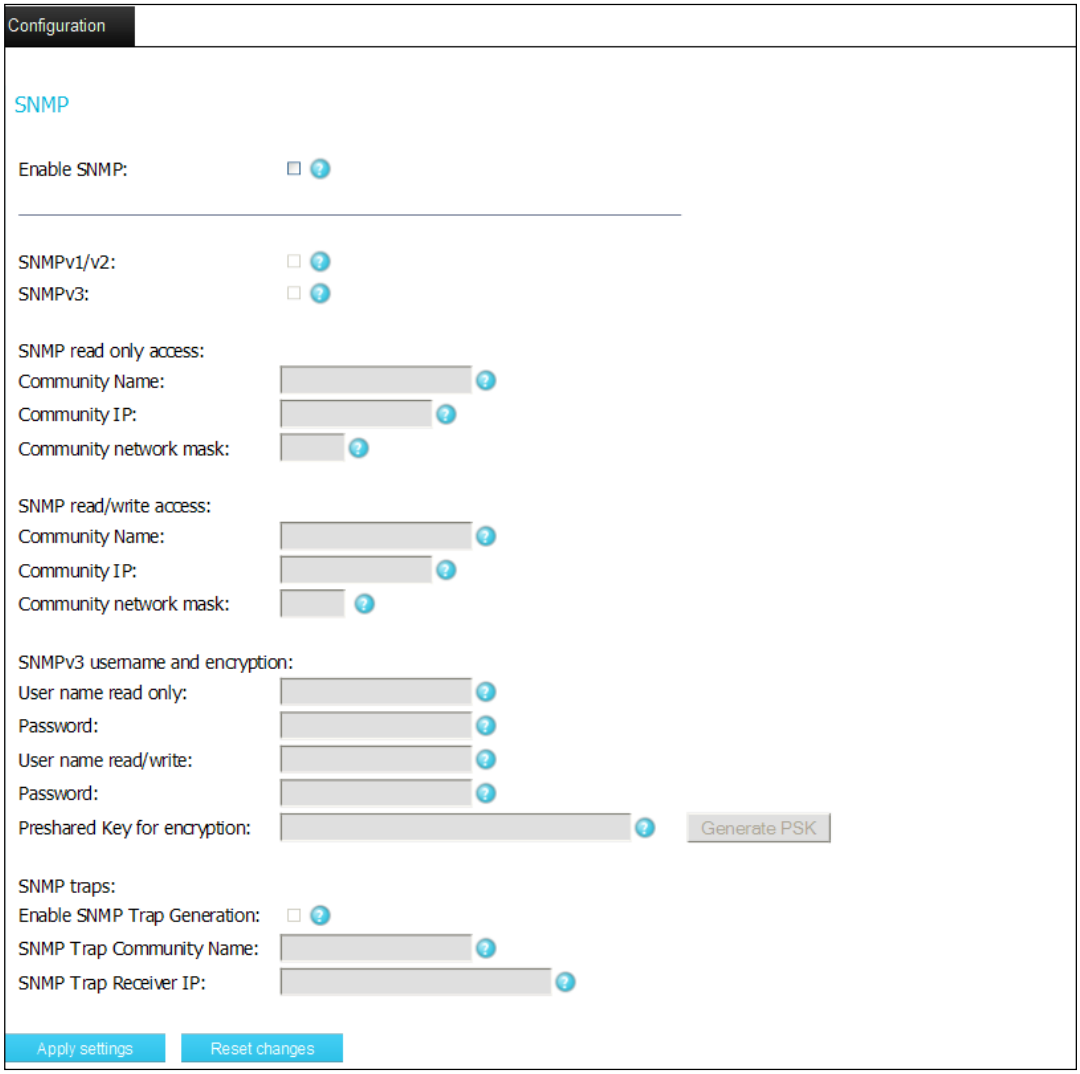
Note:

You should assign an individual certificate to each firewall for an optimum in security.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

SNMP

Using the Simple Network Management Protocol (SNMP) allows to administrate and monitor network resources like routers, switches or servers via a central location. This protocol does not only control communication between the monitored device and the monitoring station but also allows error recognition and notification.



ENABLE SNMP:

Enables or disables SNMP protocol.

SNMPv1/v2:

With SNMP activated the first or second protocol version is used. These are, however, not encrypted and thus not secure enough.

SNMPv3:

With SNMP activated, the third SNMP-protocol version is used. It provides additional protection by assigning User name and Password.

SNMP READ ONLY ACCESS / SNMP READ/WRITE ACCESS:

Note:
Select if you want to configure read-only or read/write access rights according to your requirements, and fill your data in the corresponding mask.

SNMP Community Name:

The name to be entered here is comparable with a password. Frequently used default settings are Private or Public.

SNMP Community IP:

Access to the specified Community Name is restricted to the following IP address.

Note:
If you want to allow all source IPs, select the following IP: ***0.0.0.0***

SNMP Community network mask:

Here you must enter the corresponding network mask for this IP address.

SNMPv3 USERNAME AND ENCRYPTION:

Note:
This function is available only if SNMPv3 was selected. Select if you want to configure read-only or read/write access rights according to your requirements, and fill your data in the corresponding mask.

User name:

Assign a user name for authentication with the SNMPv3 protocol.

Password:

Assign a password to your user name.

Note:
The authentication protocol used with this login is MD5.

Preshared Key for encryption:

The preshared key (PSK) is a key that consists of a combination of numbers and letters and can be used in addition to user name and password. A randomly generated number code, which may be used as a preshared key, can be created by using the "**Generate PSK**" button.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

ENABLE SNMP TRAP GENERATION:

Allows to enable/disable the SNMP trap function. With the function enabled, events like e.g. Link Up / Link Down events can be received and traced back. The firewall can trace back, from which device the message originated, because its IP address is included.

SNMP Trap Community Name:

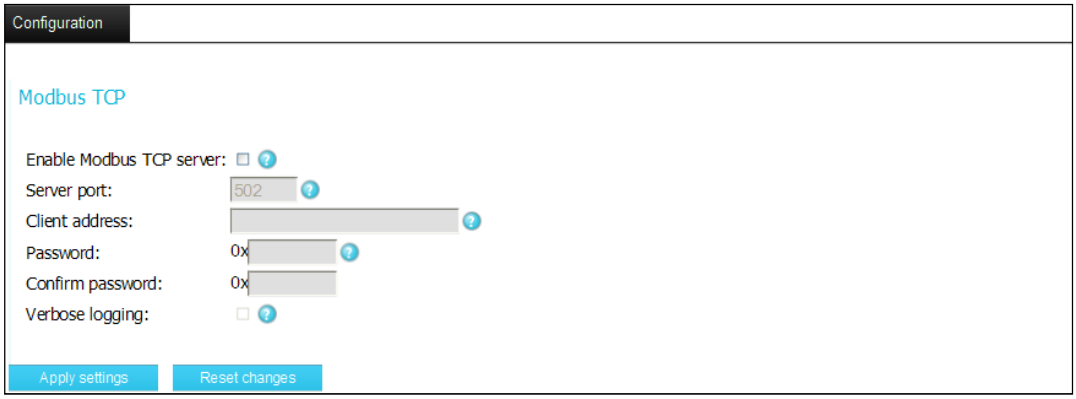
Here you enter the Community Name for traps.

SNMP Trap Receiver IP:

Enter the IP address of the trap receiver here.

MODBUS TCP

Modbus TCP allows to control the function of a device via Ethernet from a PLC unit and to retrieve status information. Communication services (Service, IPsec and Open VPN) can be controlled at the firewall and Cut & Alarm messages can be acknowledged by using this protocol.



Enable Modbus TCP server:

If the function is enabled several aspects may be controlled via Modbus TCP.

Server port:

If a specific port should be used for enquiries, it can be defined in this place. Port 502 is the default setting.

Client address:

If you want to connect a specific client and IP address or a host name can be entered. By default all clients can connect.

Password:

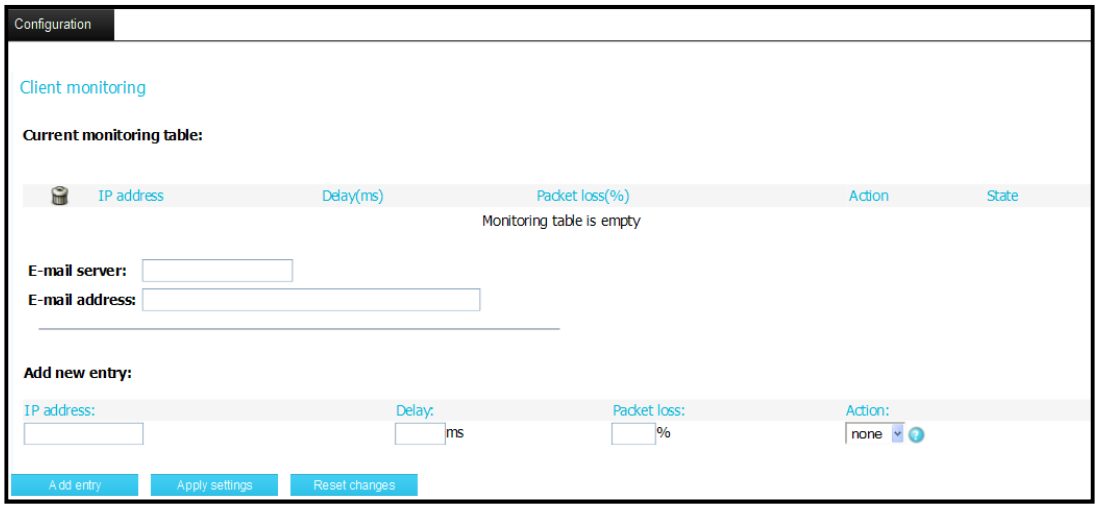
Here you can define a Password, which is prompted in the client login. This password must be re-entered in the Confirm password box.

Verbose logging:

By default, only access violations are reported. Using this option you can log additional information.

CLIENT MONITORING

The integrated client monitoring functionality is used for monitoring terminals for their availability in the network. The clients to be monitored are added to the Current monitoring table and will be checked for availability by ICMP messages in regular cycles.



A client to be monitored can initiate an activity if it is no longer available. In this case, an alarm signal or a CUT event may be initiated.

Note:

If you want to check the response time for ICMP responses you can pop up a tool tip on the LED icon in the State box.

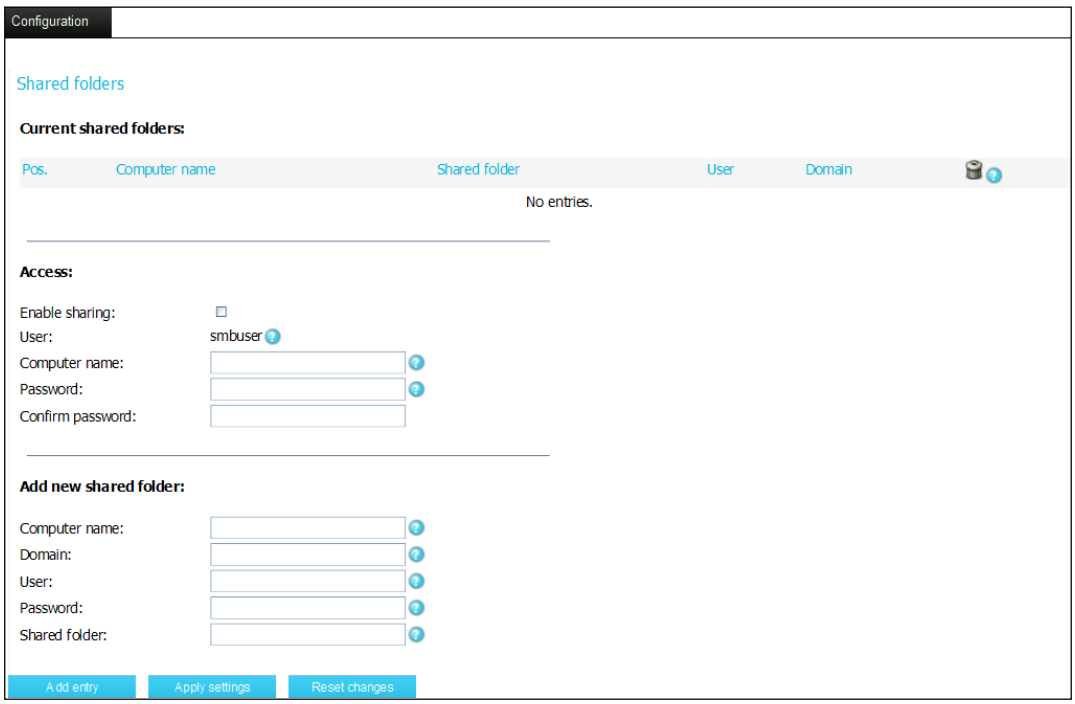
Note:

A change in state will trigger an E-mail notification if a valid address is saved in the optional E-mail server and E-mail address boxes.

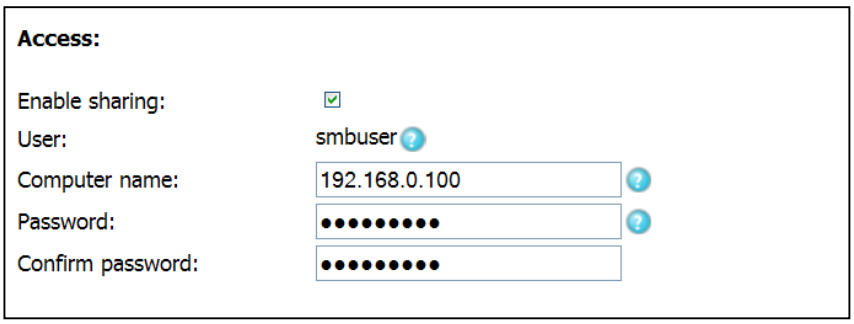
© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

SHARED FOLDERS

By using this menu item, folders can be shared, which might then e.g. be used for performing a virus scan via the firewall.

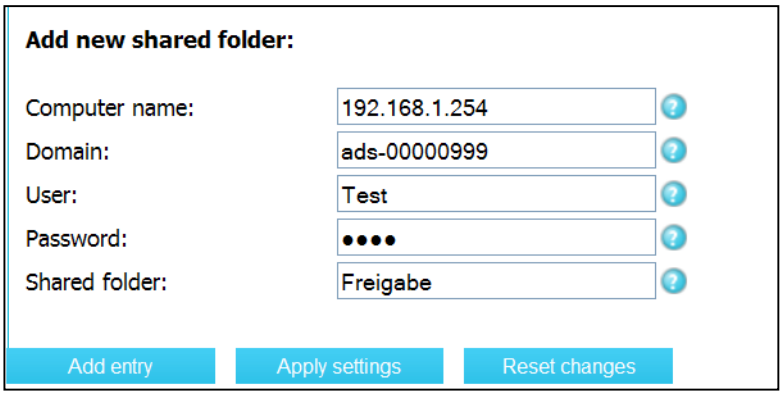


Access must be configured first in order to set up a shared folder.



You enable sharing by clicking on the checkbox. In the Computer name box you can specify the name of the computer or the IP address. Additionally, you have to specify the corresponding Password (user account password in Windows).

Access configuration can be completed by using the **Apply settings** button.



In order to set up a new shared folder, you have to enter the computer name on which the shared folder is located or the corresponding IP address in the **Computer name** box. The domain name can be entered here if the computer for sharing is part of a domain.

With the **User** and **Password** boxes, the user information will be specified, for which access to the shared folder will be permitted. The user data entered are used for limiting access to the shared folder. You enter the name of the shared folder in the **Shared folder** box.

Confirm your entry by clicking on **Add entry**.

Your shared folder will appear in the upper window section.



Note:

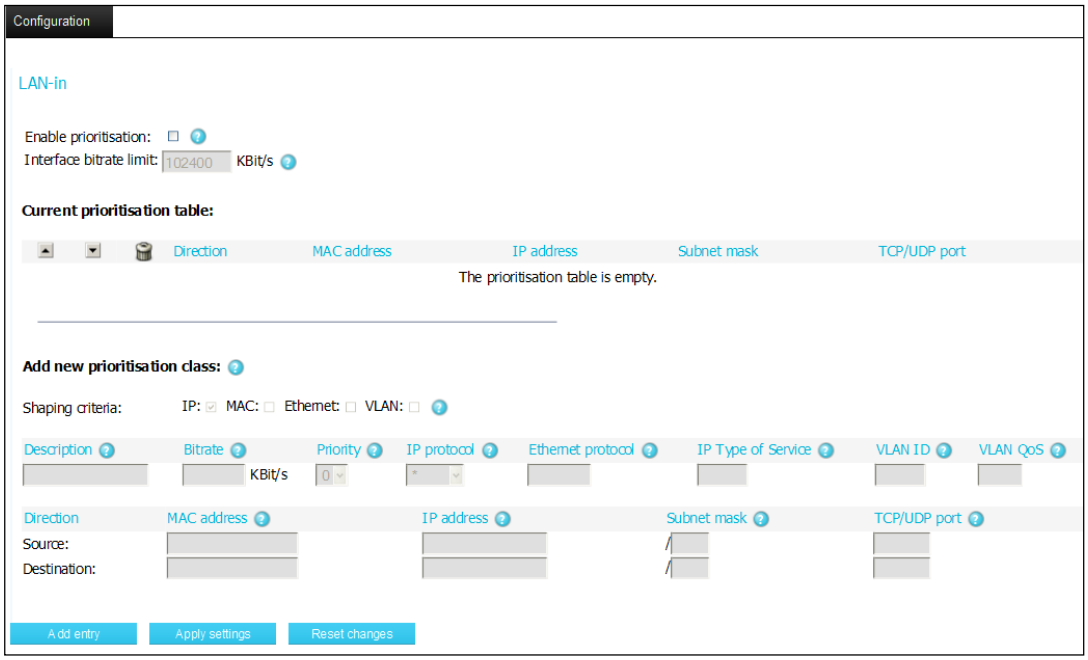
The "Shares" from the list are completely mapped to a directory on the firewall, and can then be addressed from the Explorer of the access computer by using e.g. the 192.168.0.254\|share command. This is no filtering of shares, but a collective share!

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

8.3.13 PRIORITISATION

LAN

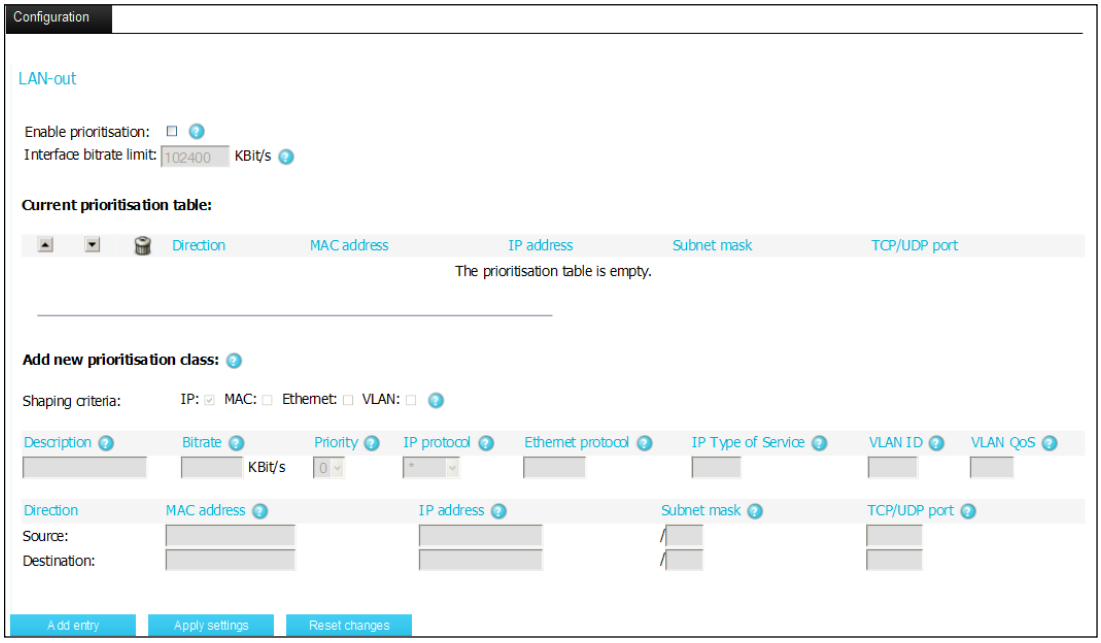
The prioritisation function integrated in the firewall is used for differentiated treatment of data flows between different interfaces. This way, it is possible to prioritise packets or to limit the bandwidth for certain protocols.

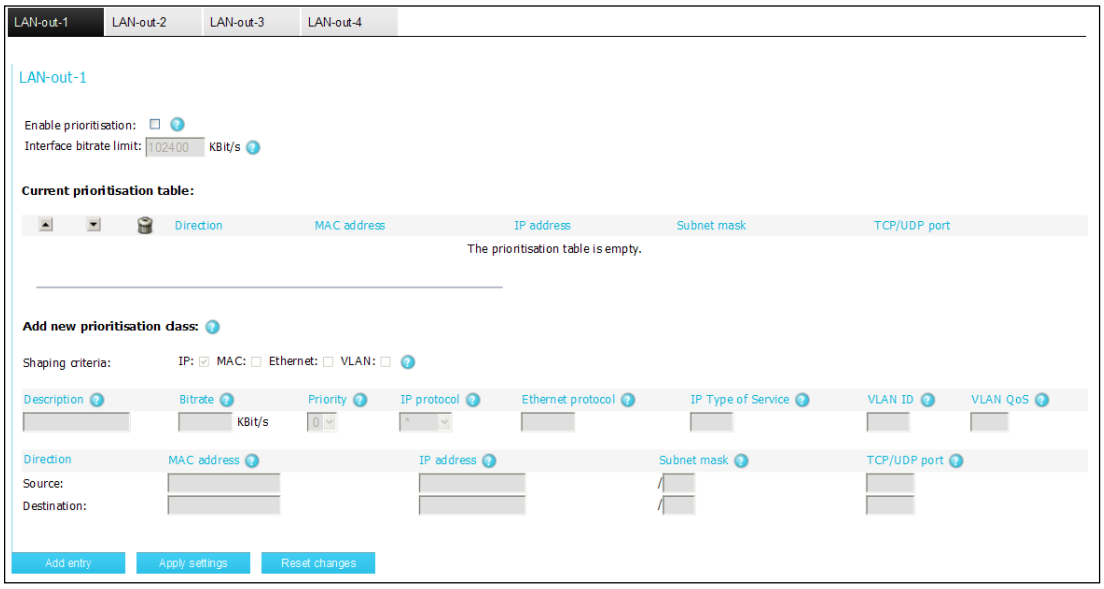


Prioritisation is enabled by entering a maximum bit rate as well as at least one prioritisation class. For instance, you'd have to enter a maximum bit rate of 51,200 Kbit/sec if the connected Ethernet infrastructure offers a maximum throughput of 50 Mbit/sec.

Criteria for prioritisation classes cannot be combined in all possible variations. Selecting IP and VLAN at the same time, is e.g. excluded by the work principle.

LAN





(IP router extended view)

LAN-out ports may be configured individually in the IP router extended mode.

Note:

*At least two classes must be created if you want to prioritise a specific data flow. The class to be created gets the lowest priority value in the **Priority** option box and so specifies the prioritised data traffic. This ensures that the prioritised data flow of the first class will have sufficient bandwidth.*

Note:

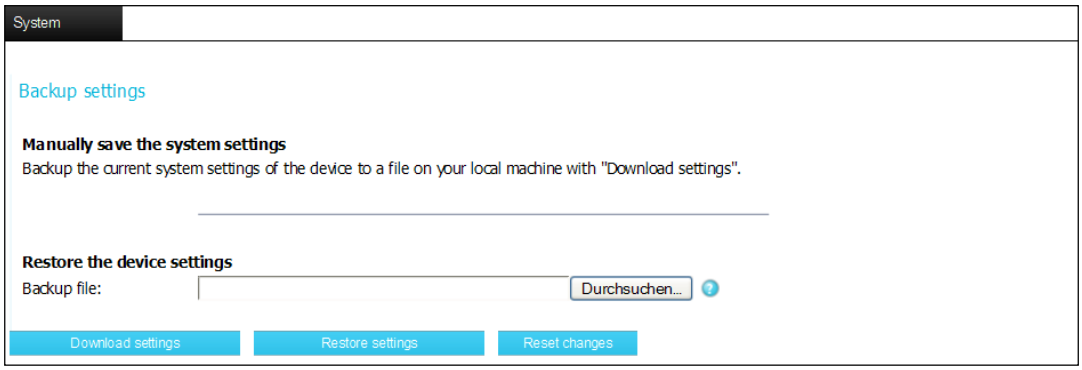
*A numerically small value in the **Priority** input box symbolises the shortest delay for Ethernet packets while a high value corresponds to a long delay!*

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

8.4 SYSTEM MAIN MENU ITEM

8.4.1 BACKUP SETTINGS

Using the backup settings you can perform a backup or recovery of the device configuration. These backups or recoveries can also be transmitted to several devices if the same firewall firmware version is used.

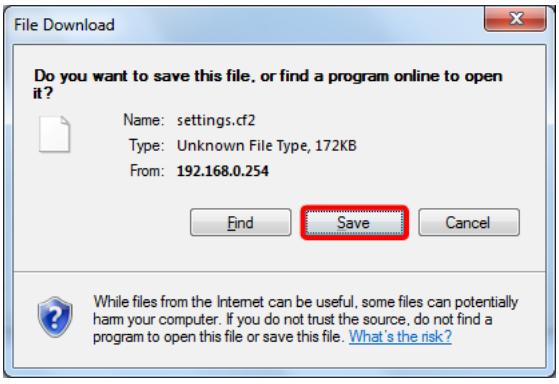


MANUALLY SAVE AND RESTORE THE SYSTEM SETTINGS

For saving your data in a file, please click on: **Manually save and restore settings in a file**.

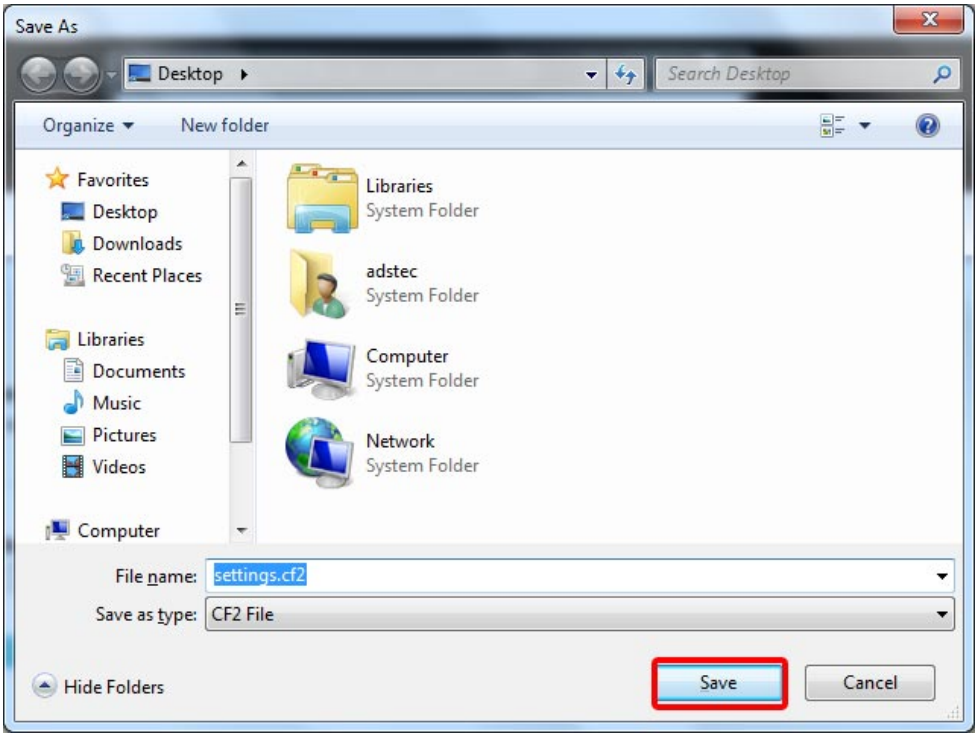
Note:

*The file name is predefined and cannot be set up in the web interface. The file name can be renamed when defining the location for saving. The file extension *.cf2 may not be changed in this case.*


File Download
Do you want to save this file, or find a program online to open it?
Name: settings.cf2
Type: Unknown File Type, 172KB
From: 192.168.0.254
Find
Save
Cancel
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

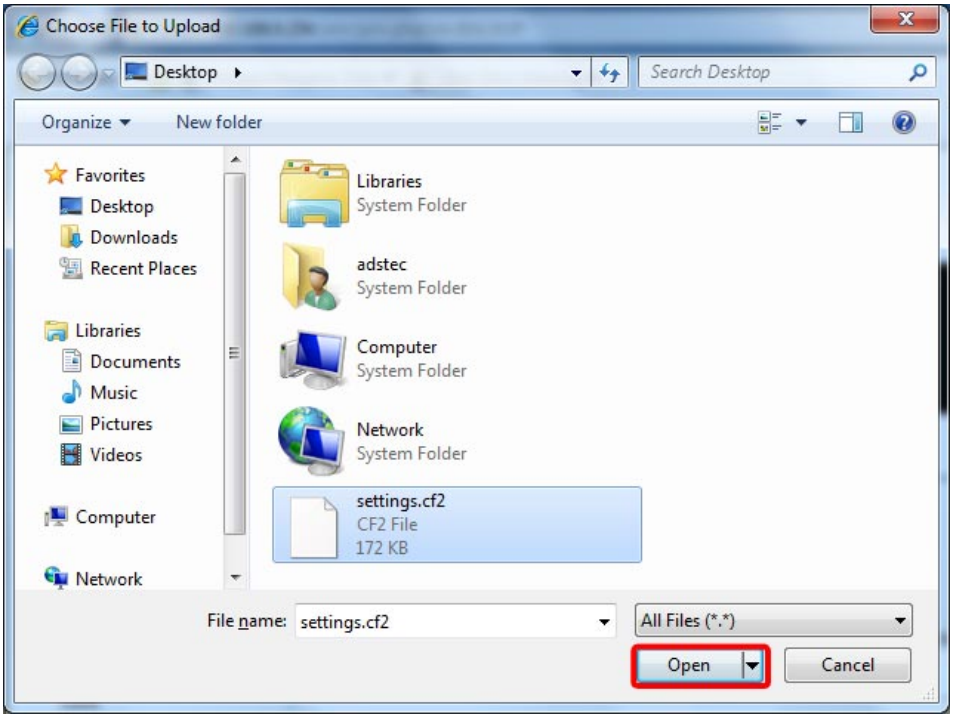
Select **Download settings**.

It asks you to save the **settings.cfg** file. Please click on **Save** and then select a location for saving. Click on **Save** one more time.



RESTORING THE DEVICE CONFIGURATION

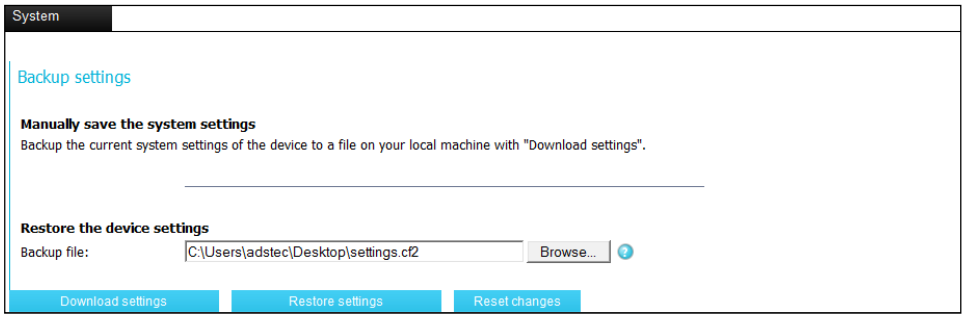
Click on **Look in** and select the **settings.cfg** file in order to load your backup settings.



Confirm this action with **Open**.

Subsequently click on the **Restore settings** button.

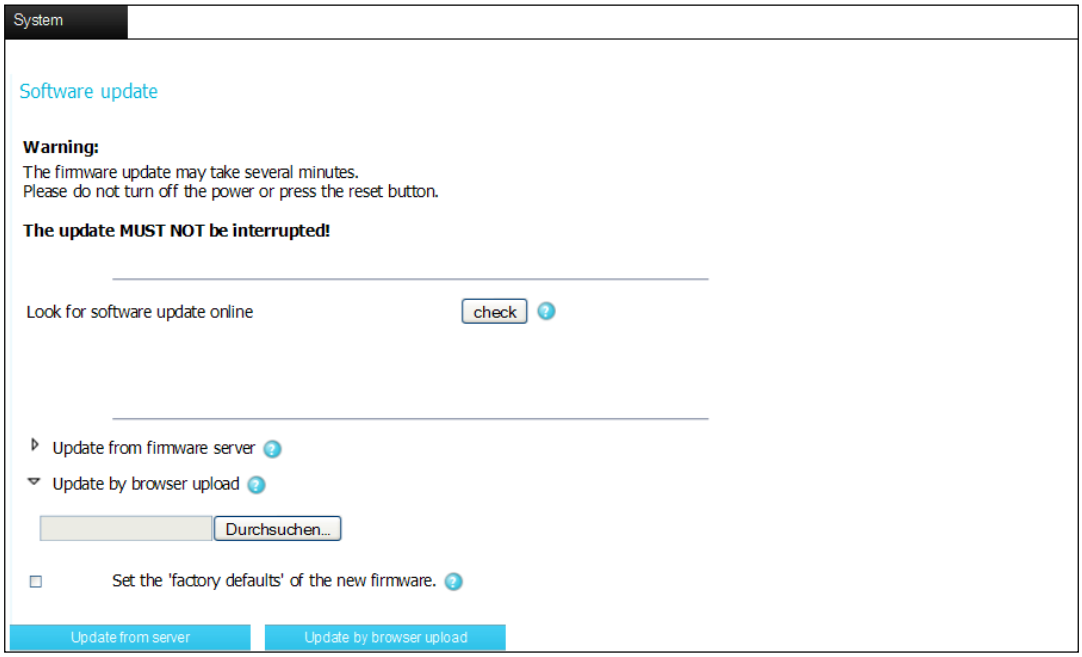
© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen



Settings will be loaded or restored after restating the device.

8.4.2 SOFTWARE UPDATE

The firewall firmware may be updated using the Software update function. This can be done in three different ways:


System
Software update
Warning:
The firmware update may take several minutes.
Please do not turn off the power or press the reset button.
The update MUST NOT be interrupted!
Look for software update online
check
Update from firmware server
Update by browser upload
Durchsuchen...
Set the 'factory defaults' of the new firmware.
Update from server
Update by browser upload

UPDATING VIA ONLINE UPDATE

By using the **Check** button, you can check whether an update is available or not. The ads-tec website must be available via the Internet in order to use this function.

UPDATING THE FIRMWARE SERVER

It is possible to update the firmware via a FTP, TFTP or HTTP server.

UPDATING VIA BROWSER UPLOAD

If the file was locally stored, the firmware file can directly be selected. Confirm your selection with **Upload via Browser Upload**.

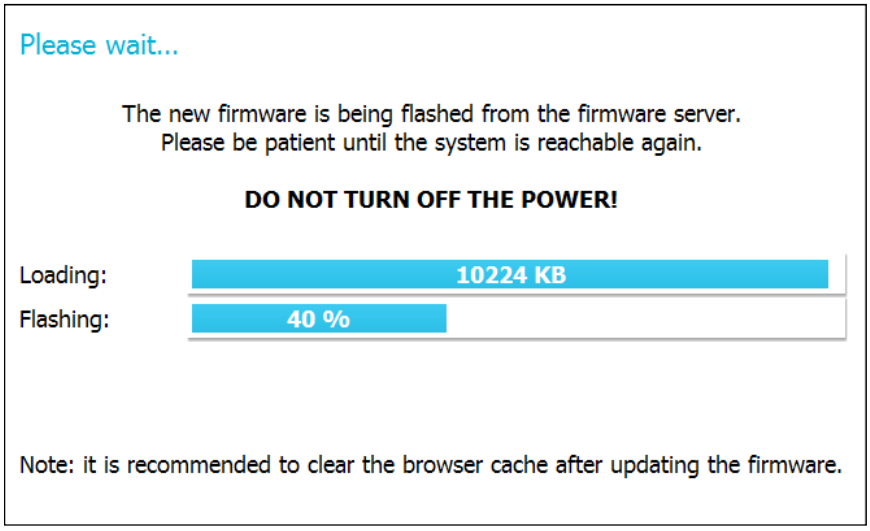
PROCEDURE:

1) Save the firmware file in a local folder of your choice on the PC.
2) Start the desired server utility or use a freeware programme like tftpd32 (available on the ads-tec service CD) in order to update your firmware. Also consider the local firewall settings on your PC so that the communication with the firewall is not barred.
3) Now, specify the folder path in which the new firmware is located under **Browse** and confirm it with **OK.**

Note:
*Be sure that the name of the firmware ends with (.bin). example: Ads-tec-IF1xxx-X.X.X-SVN-R10923M.B-7251**.bin***

4) We recommend that you select Set the factory defaults of the new firmware before starting the update process.
5) Start the update process now, by **Upload from server**.

This dialogue window will appear during the firmware update.


Please wait...
The new firmware is being flashed from the firmware server.
Please be patient until the system is reachable again.
DO NOT TURN OFF THE POWER!
Loading:
10224 KB
Flashing:
40 %
Note: it is recommended to clear the browser cache after updating the firmware.

As soon as the Link LED on the selected port lights continuously and the ACT LED is extinguished you can push the **Try to reconnect** button for confirmation.

Now the firewall will try to access the web interface. If the update process was successful the software update will be displayed.

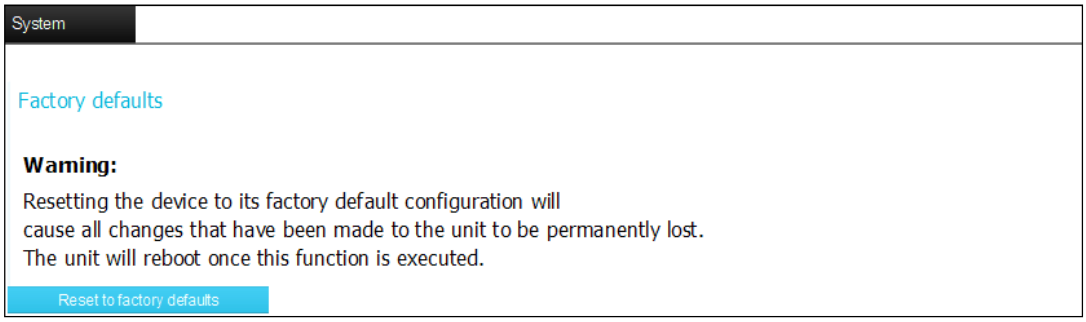
Warning:
Under no circumstances should the power supply be disrupted during this process!

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

8.4.3 FACTORY DEFAULTS

This menu item allows restoring the factory defaults by the software.

The default settings of the device will be loaded by clicking on the **Restore to factory defaults** button.


System
Factory defaults
Warning:
Resetting the device to its factory default configuration will
cause all changes that have been made to the unit to be permanently lost.
The unit will reboot once this function is executed.
Reset to factory defaults

Using the web window which will appear after that, you can click on **Try to reconnect**. The firewall will now try to access the web interface. If the update process was successful the software update will be displayed.

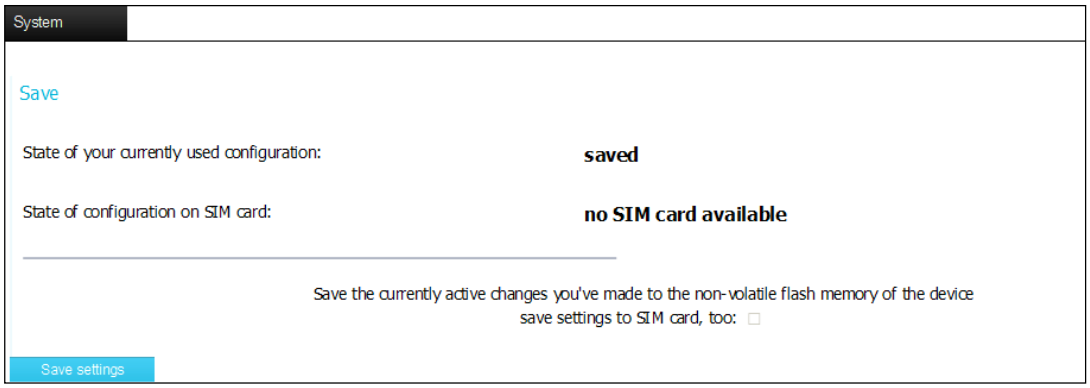
Warning:

All settings will be reset. All created filter rules will be deleted. Should you not be able to get back to the web interface after resetting to factory defaults, adapting the IP address of your PC accordingly might be required.

The following defaults are set:

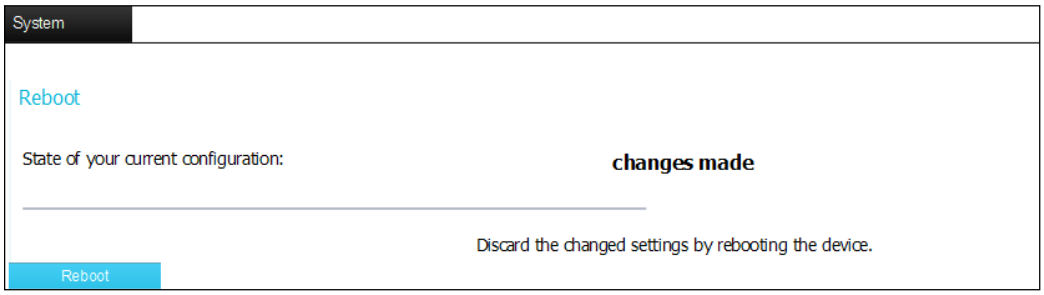
- Transparent bridge operating mode
- IP 192.168.0.254
- User name: **admin**
  Password: **admin**

8.4.4 SAVE


System
Save
State of your currently used configuration:
saved
State of configuration on SIM card:
no SIM card available
Save the currently active changes you've made to the non-volatile flash memory of the device
save settings to SIM card, too:
Save settings

All system settings made can be saved with the Save function. The settings can additionally be saved to a SIM card.

8.4.5 REBOOT



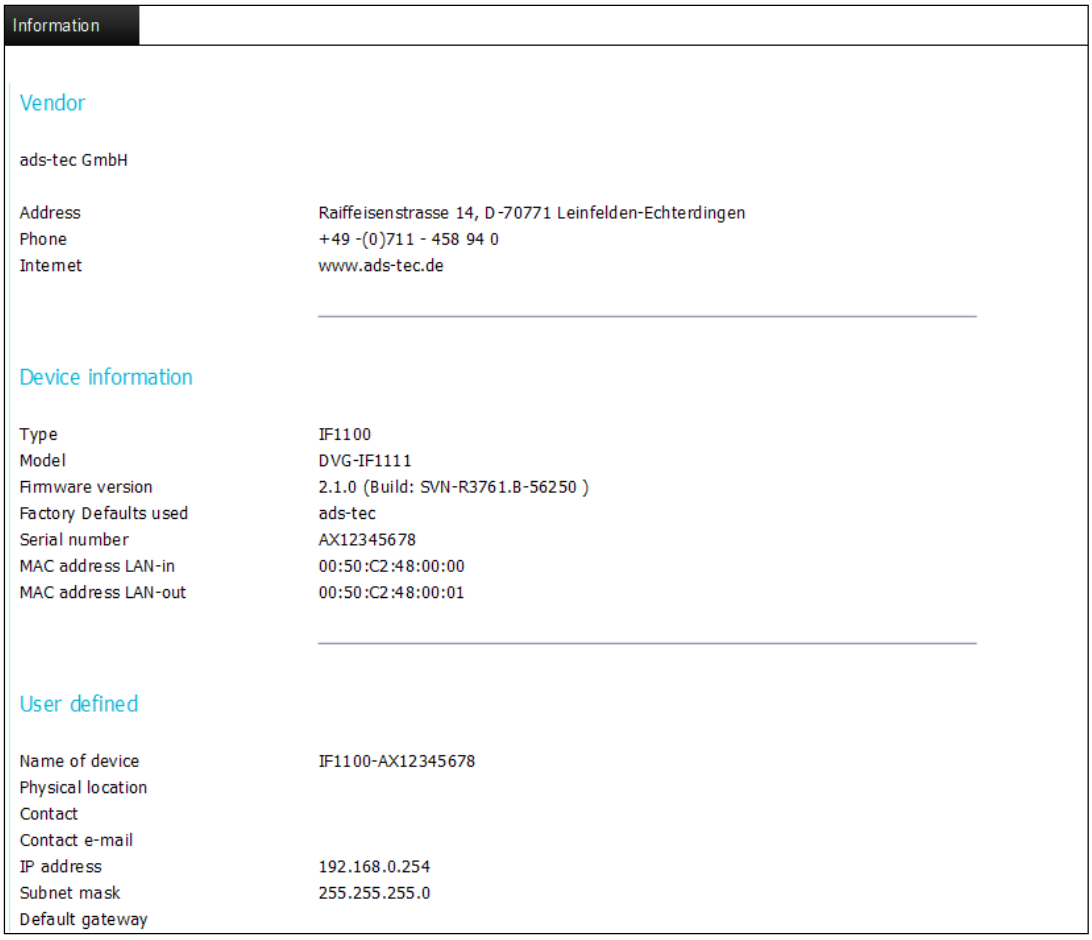
Reboots the system.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

8.5 INFORMATION MAIN MENU

8.5.1 GENERAL

The **General** menu item shows the basic device information.



VENDOR:

This box shows all relevant data about ads-tec GmbH as the manufacturer.

DEVICE INFORMATION:

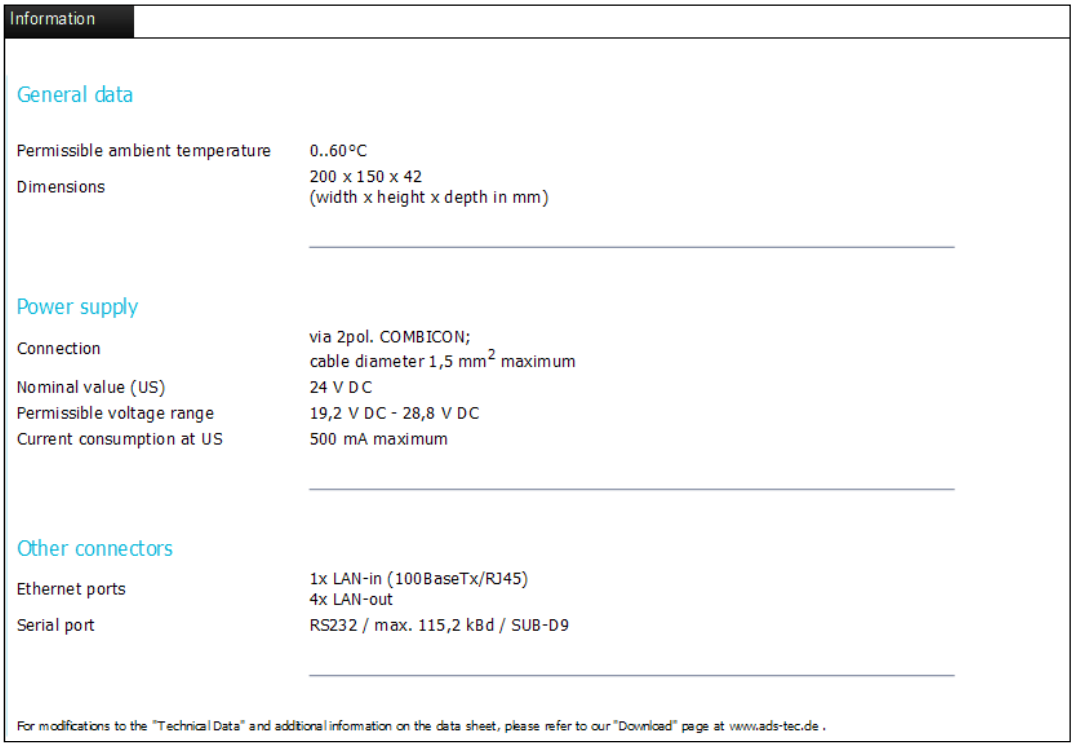
The **Device information** field shows all relevant device data like type, model and firmware version.

USER DEFINED:

The **User defined** section displays customer-specific device data.

8.5.2 TECHNICAL DATA

The Technical data screen displays General data for commissioning and the Permissible power supply data for the device.



© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

8.5.3 HARDWARE INSTALLATION

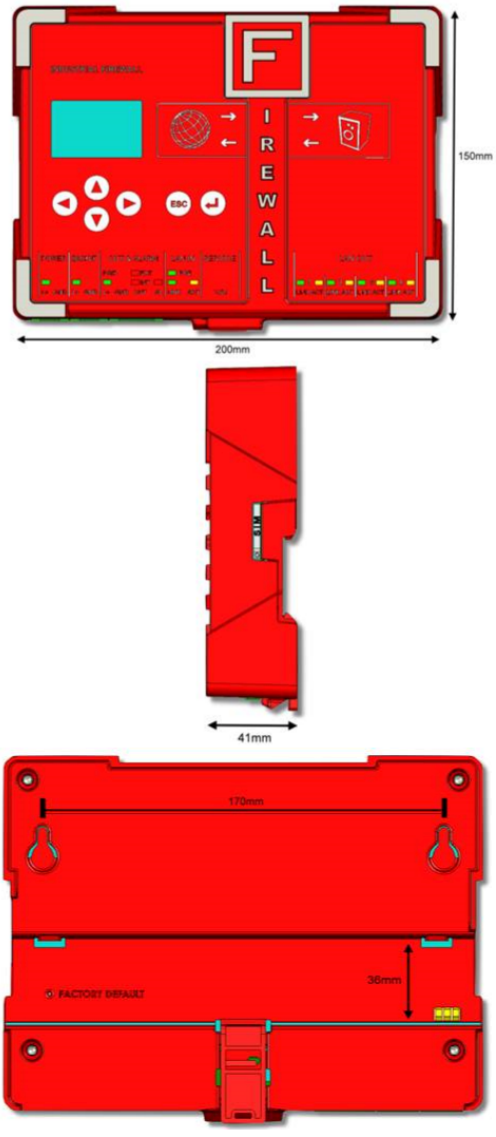
On this page you'll find which installation options are available for the firewall.

Information

Hardware installation

External dimensions

Height: 150 mm
Width: 200 mm
Depth: 41 mm



Mounting options

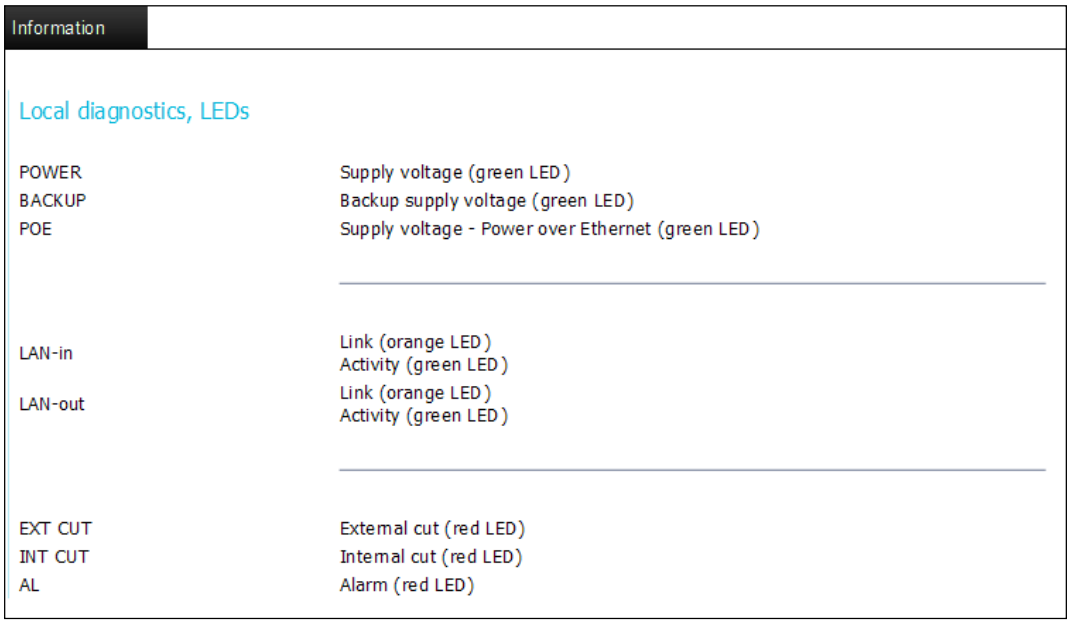
This device is suitable for DIN rail mounting and wall fastening.

DIN rail mounting

1. Set the firewall onto the upper rail.
2. Press it against the lower rail to fasten it.
3. The firewall must be locked entirely in the DIN rail!

8.5.4 LOCAL DIAGNOSTICS

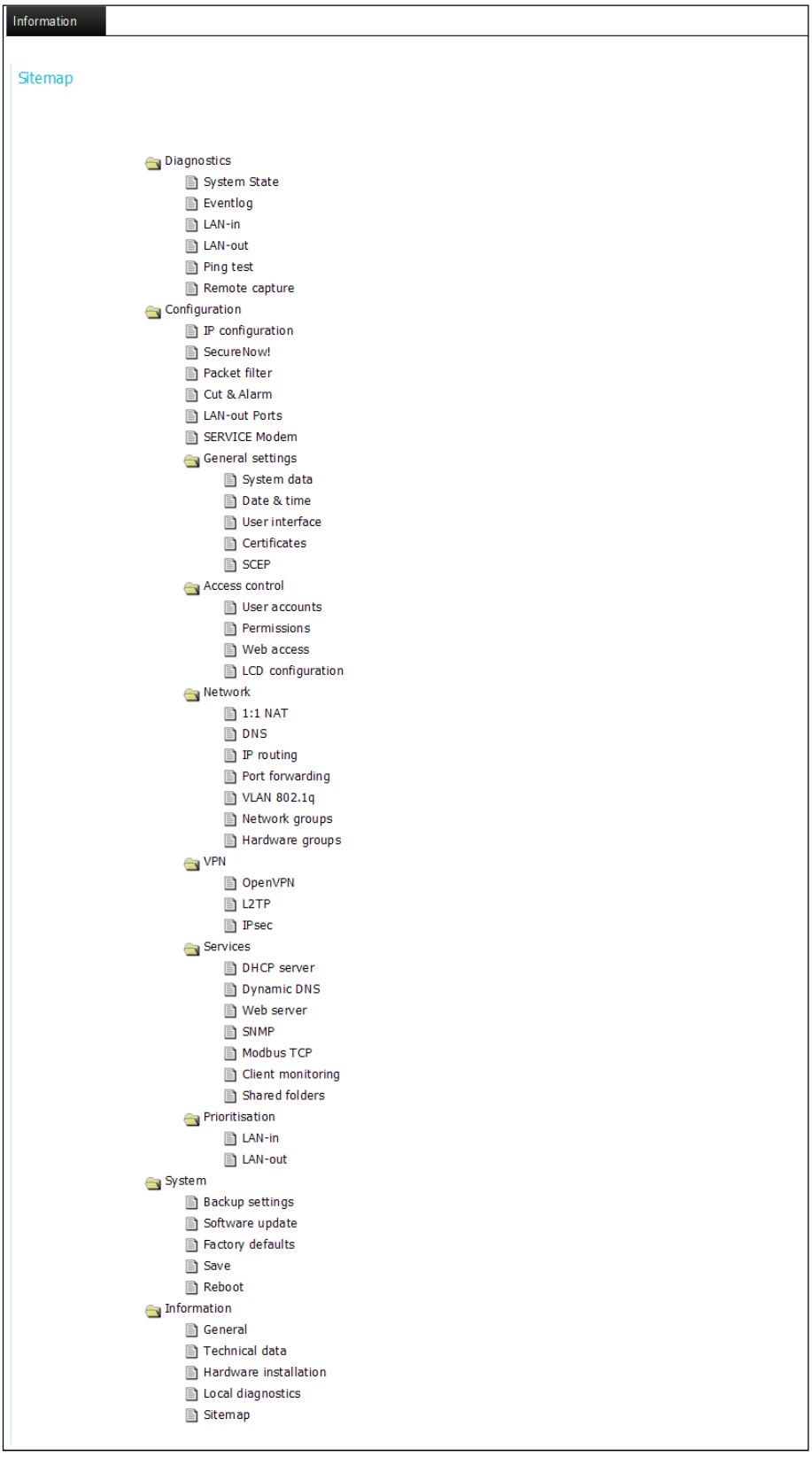
The Local diagnostics page shows the LED display functions with different system activities.



© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

8.5.5 SITEMAP

The Sitemap displays the web interface in a tree structure with all submenus for easy navigation.



9 Technical Details

9.1 Display Data

Display	Active monochrome liquid crystal display, 128x64 pixels, fully graphical, backlit

9.2 Computer Data

Hardware	Intel IXP 425 / 533MHz
Random access memory	64MB RAM
Flash memory	32MB RAM
Operating system	Embedded Linux
Configuration protocol	http, https
Keys	4 membrane keys for directional navigation and input
	1 ESC membrane key, 1 Return membrane key
Power supply	24V DC +/- 20%, redundant voltage input, PoE
CUT and Alarm	24V DC alarm output voltage supply
	24V DC feed-in of an external switching signal - galvanically isolated
	ALARM output - galvanically isolated
LAN-in	RJ45 or LWL connection 19/100MBit/s half and full duplex 100BASE-TX
	Power over ethernet in compliance with IEEE 802.3af, Class 3.
LAN-out	4x RJ45 or LWL connection 10/100MBit/s half and full duplex 100BASE-TX
Service	9-pol SUB-D connector, RS232 for connection of an external, analogue, ISDN or GPRS standard modem unit, with dial-in and dial-out functionality

9.3 General Data

External measurements	200 mm x 150mm x 41mm (B x H x T)
Weight	approx. 1 kg
Protection Class	IP20
Power consumption	max. 12 Watt (typ.)
Maximum current consumption	500 mA
Permissible ambient temperature	5° … 60°C 5° … 50°C (UL)

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

10 Service and Support

ads-tec and appointed partner companies offer you comprehensive maintenance and support services, ensuring quick and competent support should you have any questions or concerns with regard to ads-tec products and equipment.

ads-tec products may also be provided and installed by partner companies. Such devices may have customised configurations. Should any questions arise with regard to such specific settings and software installations, please contact the system supplier in question as ads-tec will not be able to reply to such questions.

ads-tec does not provide support services for any device or unit that was not bought directly from ads-tec. In any such case, maintenance and support is provided solely by the partner company that supplied the device or unit.

10.1 ads-tec Support

The ads-tec support team is available for inquiries by direct customers between 8:30am and 5:00pm, Monday to Friday. The support team can be reached via phone, fax or email.

Tel: +49 711 45894-500

Fax: +49 711 45894-990

E-Mail: mailbox@ads-tec.de

10.2 Company Address

ads-tec
Automation Daten- und Systemtechnik GmbH
Raiffeisenstraße 14
70771 Leinfelden-Echterdingen
Germany

Tel: +49 711 45894-0

Fax: +49 711 45894-990

Email: mailbox@ads-tec.de

Web: www.ads-tec.de

11 APPLICATION EXAMPLES

Note:

Below described application examples and the glossary include hyperlinks directing you to external websites. It can happen that these hyperlinks no longer work because they have been updated or are in the meantime available by using another hyperlink. ads-tec does not guarantee that any such hyperlinks to external websites work properly, and shall never be held liable for this function. Additionally, ads-tec also does not accept any responsibility or liability of any kind with respect to the installation, application and freedom from errors of any piece of Open Source software.

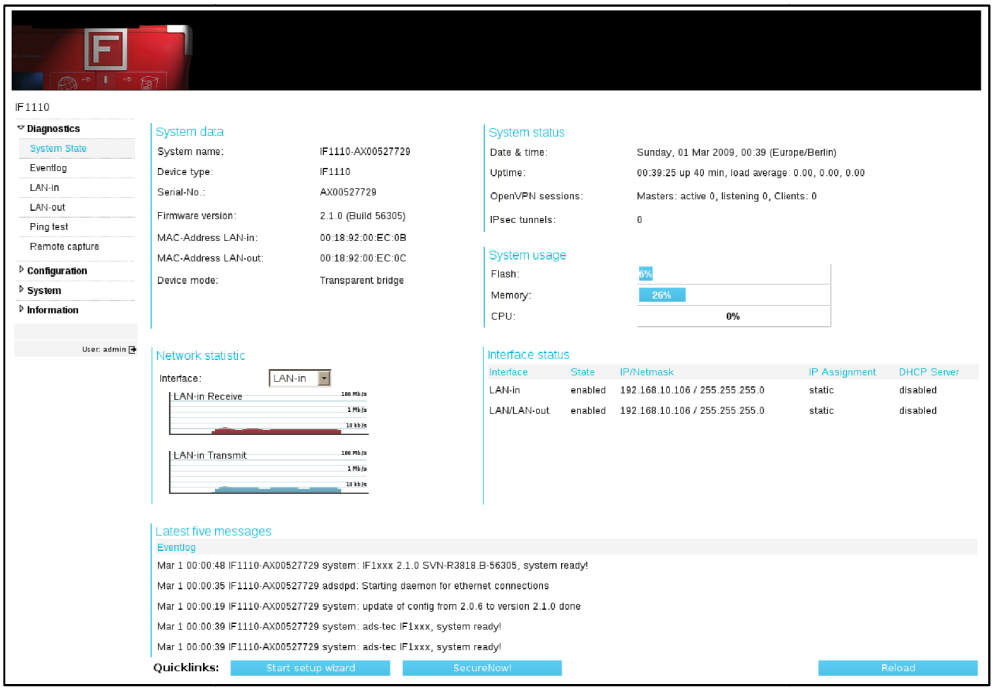
11.1 BASIC ROUTER FUNCTIONS

GENERAL

These instructions explain the most important steps for putting the IF1000 device into operation as a regular Internet router. Core items are the IP settings and the packet filter. We assume in this case that the uplink towards the Internet provider is established by using a DSL modem connected via the LAN-in interface, and that your own home network is connected with the LAN-out interface.

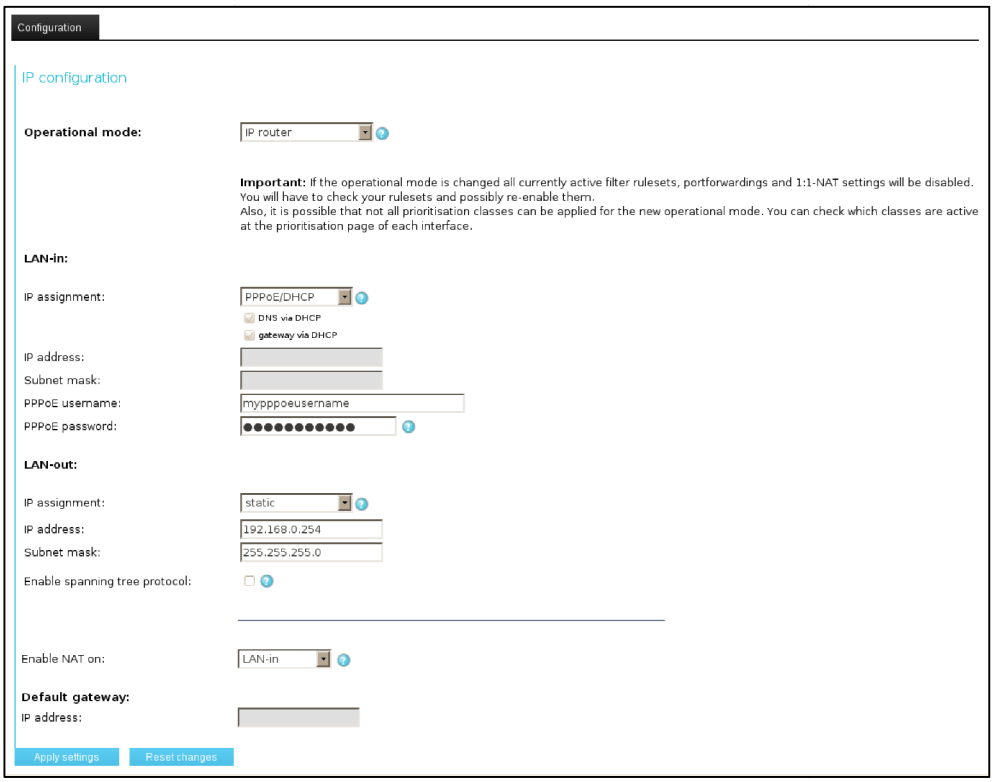
IP CONFIGURATION

The DSL modem is plugged in in the LAN-in, and the home network computer in the LAN-out connection. The firewalls default IP address is 192.168.0.254. That means that the computer which is supposed to be used for the configuration must be located within the 192.168.0.0/24 network; i.e. it must for example have IP address 192.168.0.1, and 255.255.255.0 is used as the net mask. Both user name and password for the IF1000 website, which can be opened in any browser, is admin. Your starting point is the system overview, including the essential information.



© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

If you right-click on Configuration in the main menu, you'll land on the IP configuration page. Here, you should choose the IP router operating mode. This page is then reloaded as a result, and both the LAN-in and the LAN-out interface can separately be configured. You should use PPPoE/DHCP as an assignment method for LAN-in and enter the PPPoE user name and the PPPoE password (as specified by the provider) in the respective boxes (which will then be visible). The second interface is then configured for the desired home network (as an example, the 192.168.0.0/24 default setting is retained).



Note:

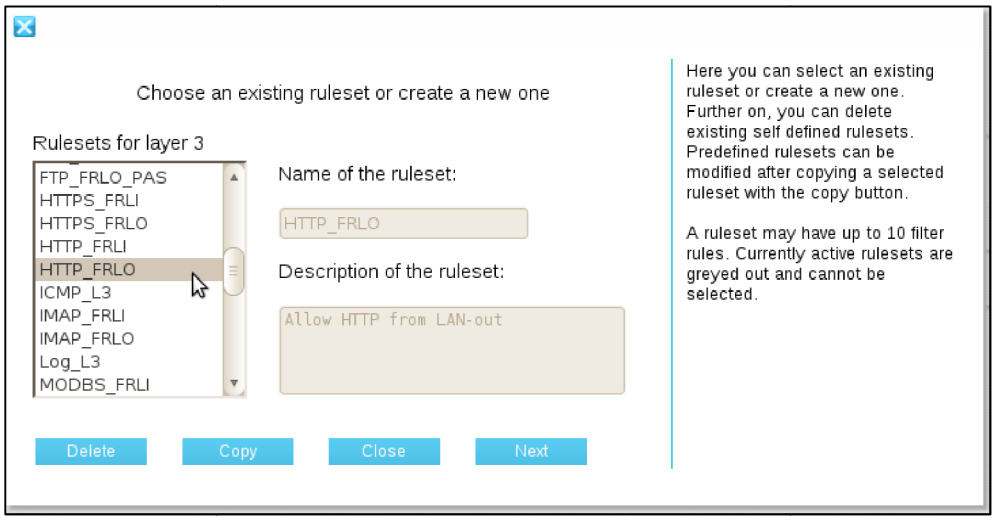
- *Should there be problems in reaching the firewall, you can read out the current operating mode and the current IP addresses from the alternating display of the LCD menu (you can skip an entry by using the ESC key).*
- *For providers without any PPPoE access information (e.g. with a cable connection), DHCP instead of PPPoE/DHCP must be used in the IP assignment for the uplink.*
- *Enabling NAT on the respective uplink interface is required for establishing a connection with the Internet. While this is done automatically with PPPoE, the setting for DHCP (e.g. with a cable provider) must be made manually.*
- *You can switch the language setting under Configuration/Basic settings/User interface.*

PACKET FILTER

The packet filter allows the firewall to be configured in such a way, for instance, that only websites (HTTP) may be accessed from the home network. You can view the active rule sets for either bridged Ethernet interfaces (layer 2, primarily for the Transbridge mode) or for autonomous IP interfaces (layer 3, i.e. for the router modes) on the overview page of the wizard under Configuration/Packet filter, and restrict the display according to the inbound and outbound interface.

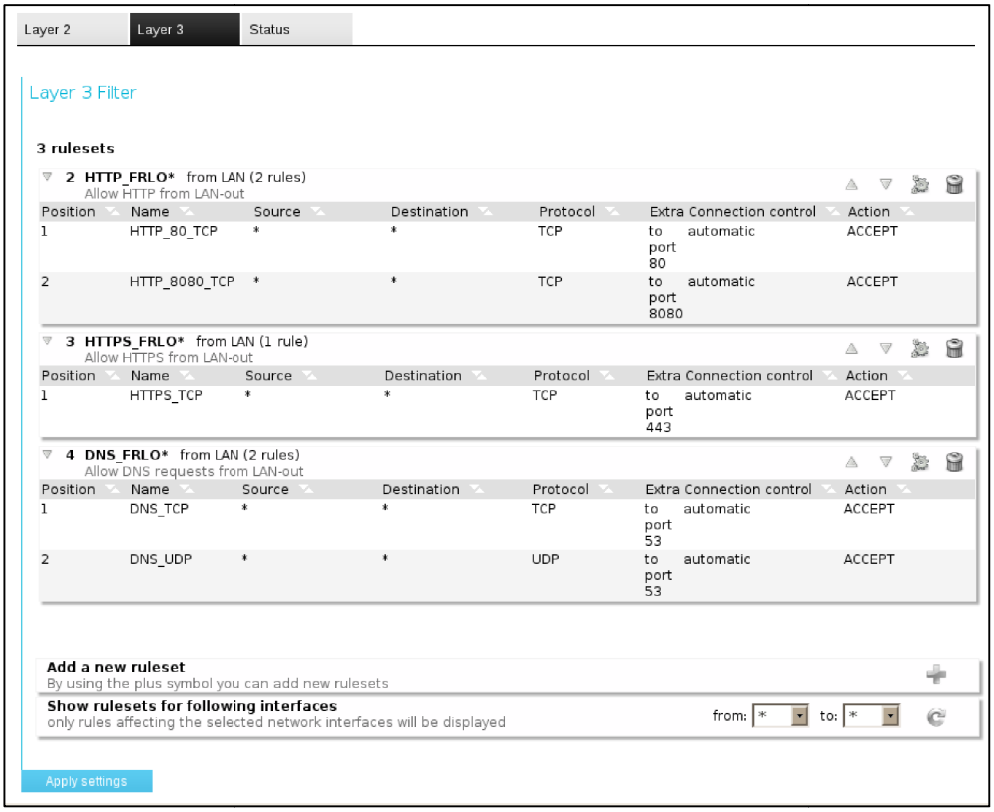


Click on Add in the Overview window for layer 3 and select HTTP_FRLO from the list of available rule sets.


Choose an existing ruleset or create a new one
Rulesets for layer 3
FTP_FRLO_PAS
HTTPS_FRLI
HTTPS_FRLO
HTTP_FRLI
HTTP_FRLO
ICMP_L3
IMAP_FRLI
IMAP_FRLO
Log_L3
MODBS_FRLI
Name of the ruleset:
HTTP_FRLO
Description of the ruleset:
Allow HTTP from LAN-out
Here you can select an existing ruleset or create a new one. Further on, you can delete existing self defined rulesets. Predefined rulesets can be modified after copying a selected ruleset with the copy button.
A ruleset may have up to 10 filter rules. Currently active rulesets are greyed out and cannot be selected.
Delete
Copy
Close
Next

Then click on Next and subsequently on Close. Add the HTTPS_FRLO rule set (for encrypted HTTP traffic) and the DNS_FRLO rule set (for Internet address resolution) in the same way. The Allow_L3 rule set (which allows all types of traffic) must be deleted by selecting this item in the list and clicking on Delete. Finally, the settings are stored by using the Apply changes button.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

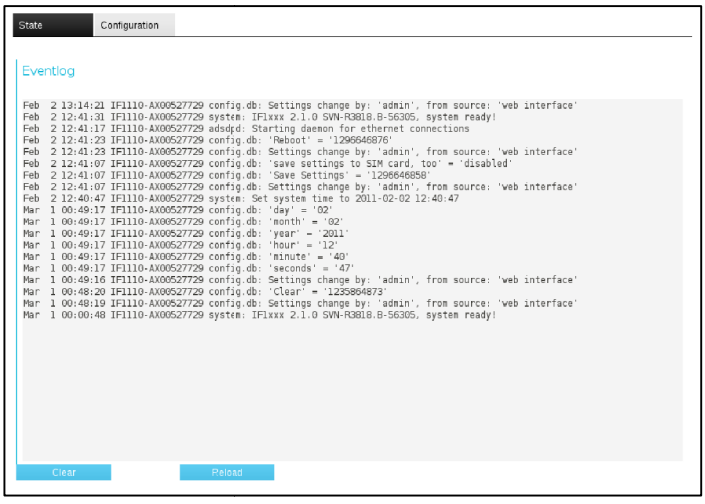

Layer 2
Layer 3
Status
Layer 3 Filter
3 rulesets
2 HTTP_FRLO* from LAN (2 rules)
Allow HTTP from LAN-out
Position Name Source Destination Protocol Extra Connection control Action
1 HTTP_80_TCP * * TCP to port 80 automatic ACCEPT
2 HTTP_8080_TCP * * TCP to port 8080 automatic ACCEPT
3 HTTPS_FRLO* from LAN (1 rule)
Allow HTTPS from LAN-out
Position Name Source Destination Protocol Extra Connection control Action
1 HTTPS_TCP * * TCP to port 443 automatic ACCEPT
4 DNS_FRLO* from LAN (2 rules)
Allow DNS requests from LAN-out
Position Name Source Destination Protocol Extra Connection control Action
1 DNS_TCP * * TCP to port 53 automatic ACCEPT
2 DNS_UDP * * UDP to port 53 automatic ACCEPT
Add a new ruleset
By using the plus symbol you can add new rulesets
Show rulesets for following interfaces
only rules affecting the selected network interfaces will be displayed
from: * to: *
Apply settings

Note:

- *An own rule set can be changed or a pre-defined rule set be viewed by using the Edit button.*
- *In order to save the changes, you either have to click on the floppy disk icon in the top bar of the menu or on Save settings under System/Save.*

EVENTLOG

The Event log under Diagnostics/Eventlog shows messages about currently running services (PPPoE connections, DHCP server, VPN, etc.).


State
Configuration
Eventlog
Feb 2 13:14:21 IF1110-AX00527729 config.db: Settings change by: 'admin', from source: 'web interface'
Feb 2 12:41:31 IF1110-AX00527729 system: IF1xxx 2.1.0 SVN-R3818.B-5630S, system ready!
Feb 2 12:41:17 IF1110-AX00527729 adsdpd: Starting daemon for ethernet connections
Feb 2 12:41:23 IF1110-AX00527729 config.db: 'Reboot' = '1296646876'
Feb 2 12:41:23 IF1110-AX00527729 config.db: Settings change by: 'admin', from source: 'web interface'
Feb 2 12:41:07 IF1110-AX00527729 config.db: 'save settings to SIM card, too' = 'disabled'
Feb 2 12:41:07 IF1110-AX00527729 config.db: 'Save Settings' = '1296646858'
Feb 2 12:41:07 IF1110-AX00527729 config.db: Settings change by: 'admin', from source: 'web interface'
Feb 2 12:40:47 IF1110-AX00527729 system: Set system time to 2011-02-02 12:40:47
Mar 1 00:49:17 IF1110-AX00527729 config.db: 'day' = '02'
Mar 1 00:49:17 IF1110-AX00527729 config.db: 'month' = '02'
Mar 1 00:49:17 IF1110-AX00527729 config.db: 'year' = '2011'
Mar 1 00:49:17 IF1110-AX00527729 config.db: 'hour' = '12'
Mar 1 00:49:17 IF1110-AX00527729 config.db: 'minute' = '40'
Mar 1 00:49:17 IF1110-AX00527729 config.db: 'seconds' = '47'
Mar 1 00:49:16 IF1110-AX00527729 config.db: Settings change by: 'admin', from source: 'web interface'
Mar 1 00:48:20 IF1110-AX00527729 config.db: 'Clear' = '1235864873'
Mar 1 00:48:19 IF1110-AX00527729 config.db: Settings change by: 'admin', from source: 'web interface'
Mar 1 00:00:48 IF1110-AX00527729 system: IF1xxx 2.1.0 SVN-R3818.B-5630S, system ready!
Clear
Reload

11.2 Establishing an Open VPN connection

General

By using OpenVPN, you can exchange data even beyond the borders of a complex transmission network (e.g. by using the Internet) like inside a (virtual) internal LAN. In order to do so, all subnets, which together define the virtual LAN, are connected by an Open VPN tunnel between an OpenVPN server (Server) and an OpenVPN client.
The firewall may either be configured as an OpenVPN Server or as an OpenVPN client. SSL certificates are used for authentication and encryption of this connection. The most important VPN applications are "Site-To-Site VPN" and "Site-To-End VPN" - these will be explained in this document by using examples.

The ads-tec IF1000 series supports OpenVPN, because it excels, thanks to its simple usability and its smooth establishment of connections beyond any routing and NAT borders. Subnets on Ethernet level (OSI layer 2) or on IPv4 level (layer 3) can be connected with each other by using OpenVPN. In layer 2 mode, transmitted data is independent on the IPv4 protocol - this means that the data can also be purely Ethernet based data.

Ethernet (layer 2) and IPv4 (layer 3) tunnel mode

In layer 2 mode, all OpenVPN connections at the LAN-out interface together with their physical connections (in IP router mode) or all OpenVPN connections at the LAN-out interface (internal traffic) (in extended IP router mode) are connected as an Ethernet bridge. Data traffic can be filtered on layer 2 level.
Layer 3 OpenVPN connections, on the other hand, always have their own independent virtual interface, which must be set up in the Configuration →IP configuration menu item. Only IPv4 data traffic can be transmitted by using these connections. The layer 3 packet filter (Configuration → Packet filter) is then to be used for filtering the inbound and outbound data traffic of the tunnel.
The tunnel mode to be used for a certain connection must be defined by using the "Layer" option when adding a new connection.



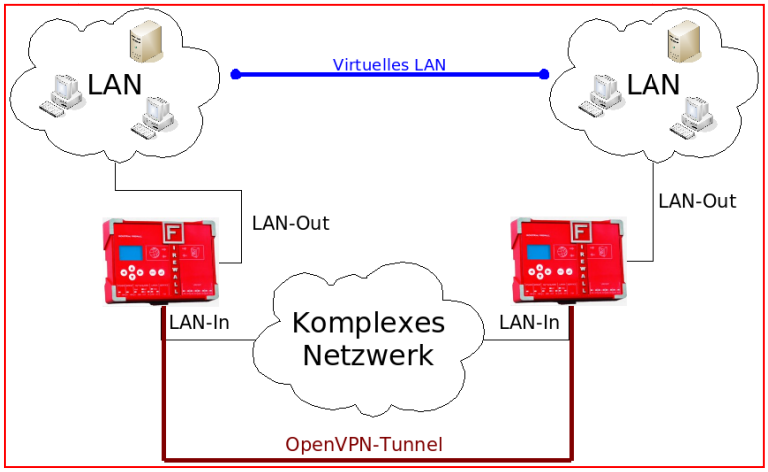
Note:

There are some certificates pre-installed for testing purposes on the device. These certificates must never be used for the final configuration, since they cannot ensure an unambiguous authentication. Instead it is essential to generate your own certificates. We recommend that you delete the demo certificates before any use in production. With respect to this, please refer to our use case "Certificates".
The IF1000 series is always using DHE-RSA-AES128-SHA as a fixed TLS cyphering algorithm. This provides for an optimum performance of the crypto hardware acceleration and for higher security as well. Please make sure that no different algorithm is set up in the remote device, if you connect the device with another OpenVPN device.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

SITE-TO-SITE VPN

With a site-to-site VPN, two remote subnets are connected to a single virtual LAN by using two VPN routers (e.g. two local networks of two very remote locations of the same company). In the IF1000 series IP router mode, the transmission network located between the routers (e.g. the Internet) is connected with the corresponding LAN-in interface, while the computers of the local networks are connected with the LAN-out interface. One of the firewalls is configured as an OpenVPN Server, while the other one is configured as an OpenVPN client, which establishes the connection with the Server firewall (see below).
In IP router extended mode or when using layer 3 OpenVPN connections, both firewalls don't unconditionally have to be connected via the LAN-in interfaces. But we'll come back to that later.

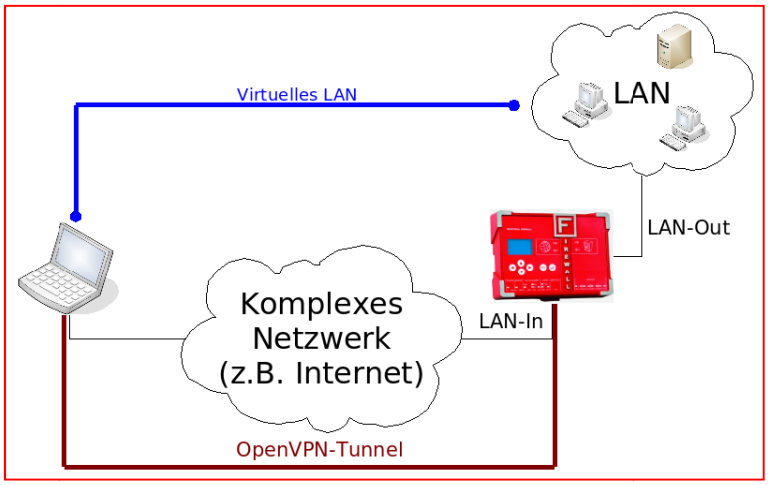


Note:

Should the complex transmission network consist of several subnets, you'll have to ensure that a dedicated route for IP packets exists between both VPN endpoints!
In our example, both devices must be configured as an IP router.
In order to make sure that the computers of both subnet LANs can reach each other, they must be located within the same subnet (e.g. 192.168.1.0/24).

SITE-TO-END VPN

With site-to-end VPN, a single computer is connected with a firewall (e.g. a remotely working employee is connected with the company network by using the Internet). The external computer is connected to the firewall via the LAN-in interface (e.g. via DSL) and the company internal LAN is connected via the LAN-out interface. Both the firewall, as well as the PC, may work as the OpenVPN Server (while the remote terminal must be configured as a client, each time).



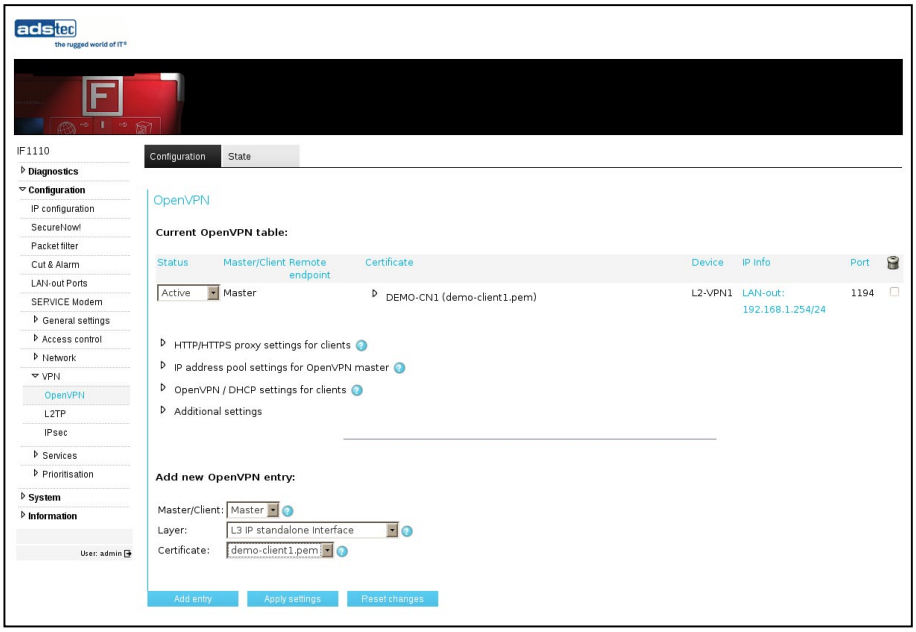
Note:

Should the complex transmission network consist of several subnets, you'll have to ensure that a dedicated route for IP packets exists between both VPN endpoints!
In our example, both devices must be configured as an IP router.
In order to make sure that the computers of both subnet LANs can reach each other, they must be located within the same subnet (e.g. 192.168.1.0/24).

LAYER 2 OPENVPN SERVER CONFIGURATION

For the device to be configured in Server mode (e.g. with 192.168.0.254 as an IP address for LAN-in and with 192.168.1.254 for LAN-out), the options "Server", "Layer: L2 Ethernet" as well as a certificate have to be selected. An OpenVPN Server connection entry is created by using "Add", and the local port is automatically assigned in the process. The port number is essential for the client configuration, since the client must establish a connection with this port (numbers start from 1194 and consecutive).
The new connection now appears in "Current OpenVPN entries" with the IP configuration of the "LAN-out" interface (or the LAN-out interface) being displayed in the interface "IP info" column.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

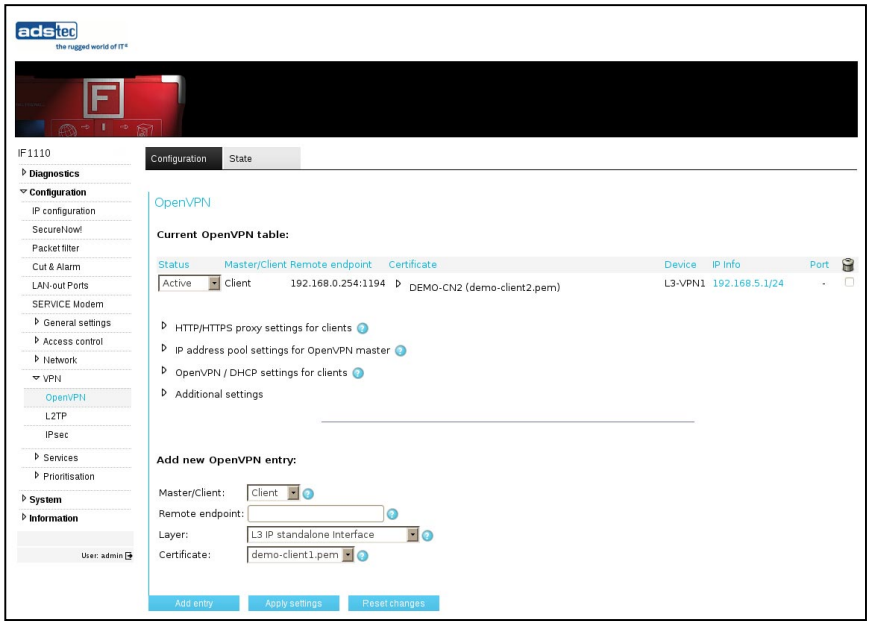


Note:

Server and client certificates must have been signed by the same CA (certificate authority). The related CA certificate must be available at both endpoints of the connection, and is then automatically used for verifying the client certificates of the corresponding remote terminal.
A maximum of 10 OpenVPN connections is possible.

LAYER 2 OPENVPN CLIENT CONFIGURATION

The "Client" mode is now selected for the device to be configured in client mode (e.g. with 192.168.0.1 as an IP address for LAN-in and with 192.168.1.1 for LAN-out). The IP address of the OpenVPN Server followed by ":" and by the port number of the VPN server is specified as the VPN remote endpoint. The "Layer" option must be set to "L2 Ethernet". The endpoint definition is added by using "Add" and the OpenVPN tunnel is directly established.
The new connection now appears in "Current OpenVPN entries" with the IP configuration of the "LAN-out" interface (or the LAN-out interface) being displayed in the interface "IP info" column.



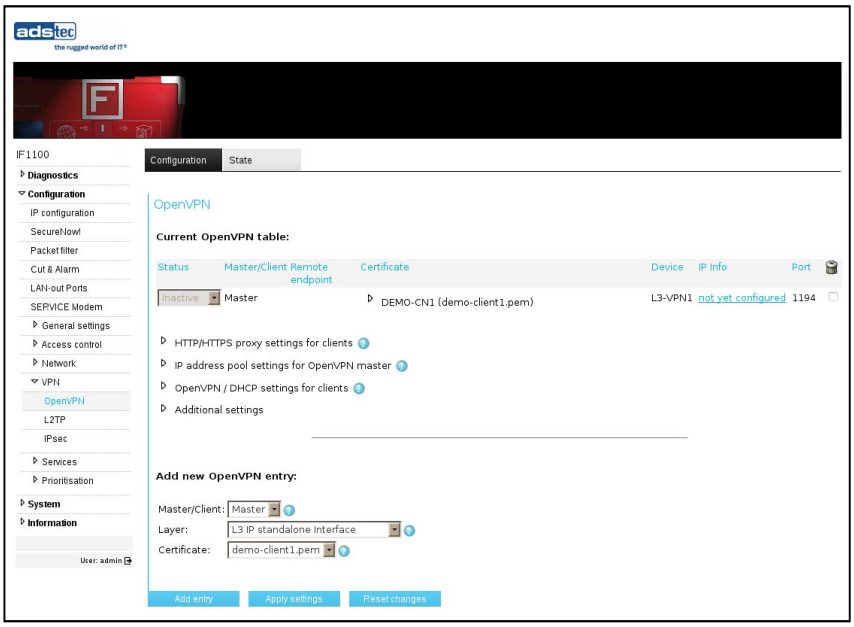
Note:

If the client is located behind a proxy server, the HTTP proxy settings must be enabled in the "HTTP/HTTPS proxy settings for clients" menu item. Then you'll be able to specify IP address and port, as well as username and password for the proxy.

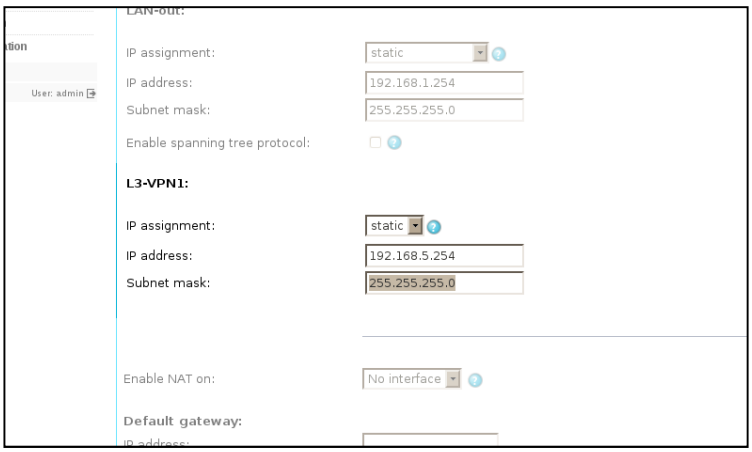
© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

LAYER 3 OPENVPN SERVER CONFIGURATION

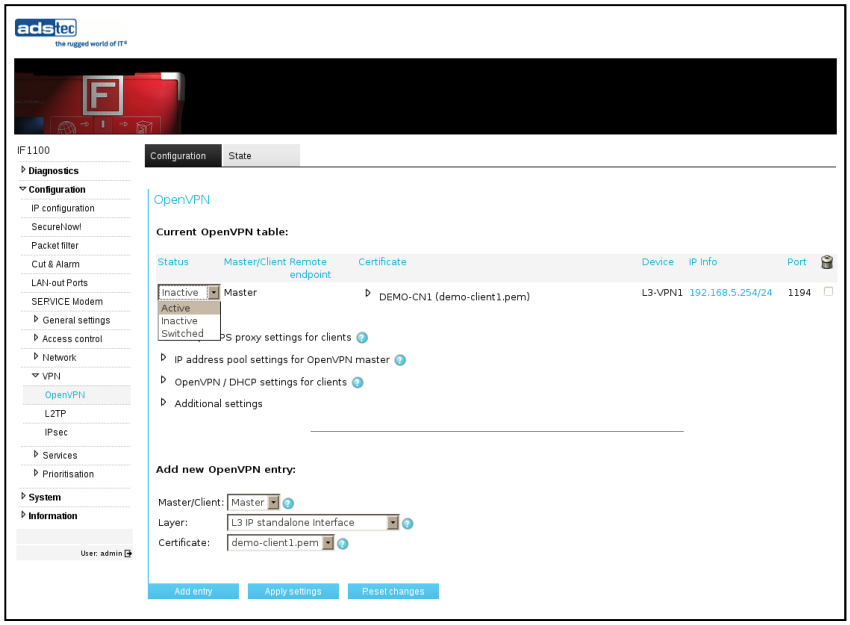
The "Server" mode and a certificate are selected for the device to be configured in Server mode. An OpenVPN Server connection entry is created by using "Add", and the "Layer: L3 IP interface" option is applied in this case.



The new connection now appears in the "Current OpenVPN entries" menu item, where the ""Interface IP info" column shows that the related L3 VPN interface does not have a valid IP configuration at this point in time. A single click on the note text will guide you to the "Configuration ☐ IP configuration" page, where an IP address and a net mask must be specified for the matching L3 VPN entry.

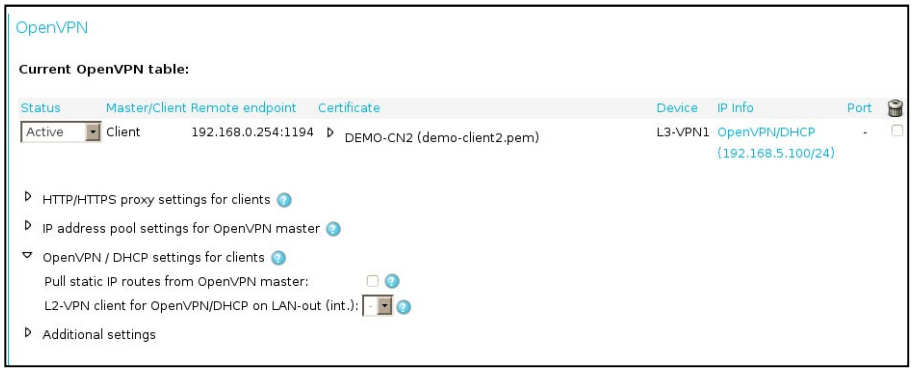


Once the IP is configured, the IP setting is visible on the OpenVPN page. All that's left to do now is setting the VPN connection status from "Inactive" to "Active".



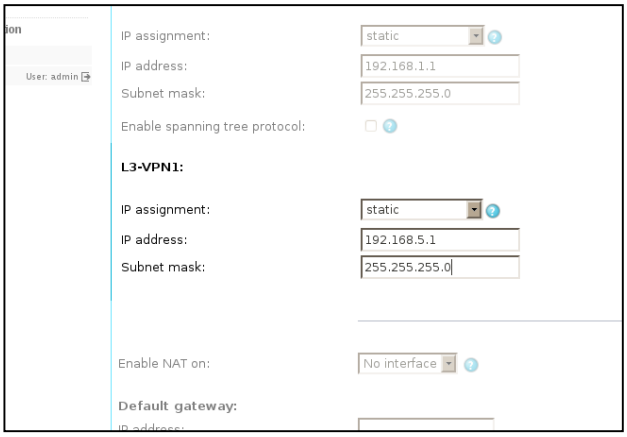
LAYER 3 OPENVPN CLIENT CONFIGURATION

For the device to be configured in client mode, the option "Client" and "Layer: L3 IP interface" is selected when adding the new connection. The IP address of the OpenVPN Server followed by ":" and by the port number of the VPN server is specified as the VPN remote endpoint. The endpoint definition is then added by using the "Add" button, and the OpenVPN tunnel is directly established with the "OpenVPN/DHCP" default setting. As a result, no further IP configuration is required as long as the server assigns the IP addresses per OpenVPN method. Configuration with dynamic IP addresses is explained in more detail in the next chapter.

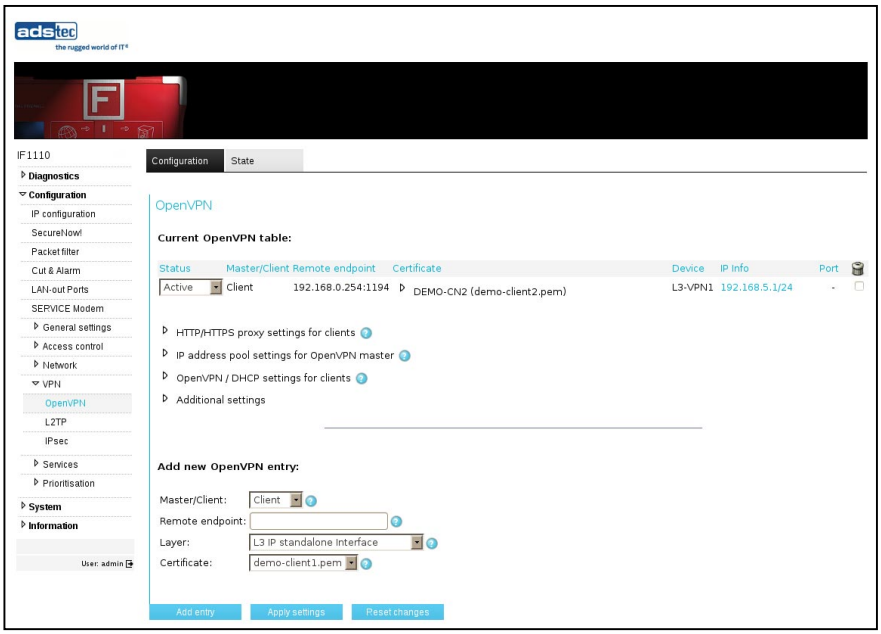


In all other cases, the IP address and net mask of the L3 VPN interface must be set up in the Configuration☐ IP configuration menu item.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen



Subsequently, the statically assigned IP address is visible on the OpenVPN page.

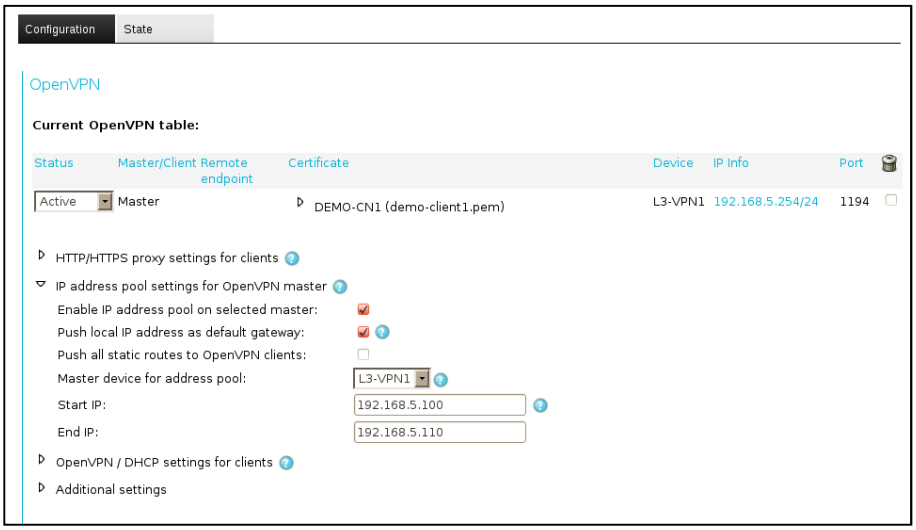


OpenVPN with dynamic IP addresses

OpenVPN offers the opportunity of having IP addresses assigned to an OpenVPN client by an OpenVPN Server. This works similar to the DHCP method, but with a specific OpenVPN protocol. Settings must be made for both the Server and the client device in order to use this option.

Server device settings

The "Enable IP address pool on selected Server" function must be enabled at the Server device. An interface for the existing connections has to be selected if several Server connections are created. As a result, this function can only be used for one of the 10 connections possible at max.
In the example, the Server is now to assign IP addresses from the LAN-out range of addresses. Additionally, the Server device is in "Extended IP router" mode in the example, which has the result that the VPN connections on the LAN-out (internal) interface are bridged, and not connected with the LAN-out ports on Ethernet level (but on IPv4 level by means of routing).
Selected IP addresses are e.g. 192.168.5.100-110 corresponding to a valid address range of the LAN-out (internal) or L3 VPN interface.

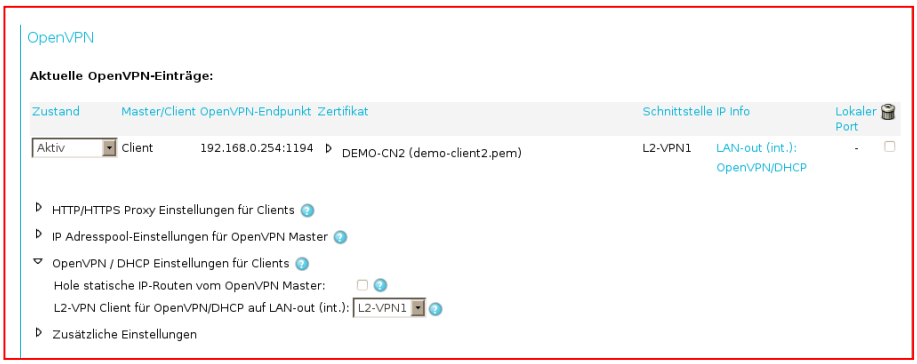


Furthermore, the Server device can also offer its services as a default gateway ("Push local IP address as default gateway" option), or the static routes configured in Configuration ☐ Network ☐ IP routing can be transmitted to the client ("Push all static routes to OpenVPN clients" option).

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

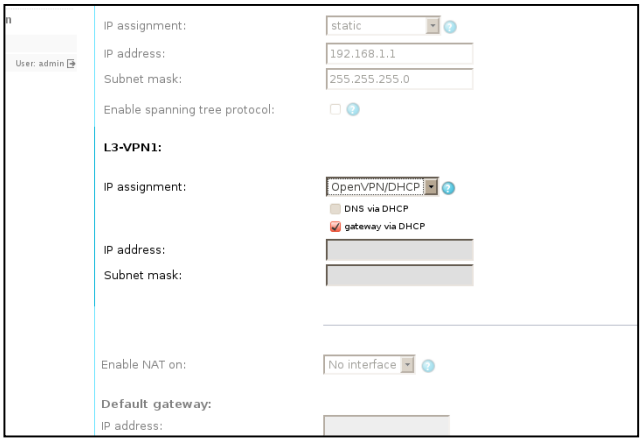
CLIENT DEVICE SETTINGS

The options in the "OpenVPN / DHCP settings for clients" window must be enabled for the client. If a layer 2 connection is used, the corresponding interface must be selected for the "L2 VPN client for OpenVPN/DHCP on LAN-out (int.)" setting. This is only possible for one layer 2 connection of 10 connections usable at max.



With a layer 2 OpenVPN connection, the protocol of the LAN-out interface (in IP router mode) or of the LAN-out internal interface (in IP router extended mode) must now be configured at the client device on the "IP configuration" page, and set to "OpenVPN/DHCP". If the Server acts as the default gateway, like in our example ("Push local IP address as default gateway" option), the "Gateway via DHCP" option can additionally be enabled in this menu item.

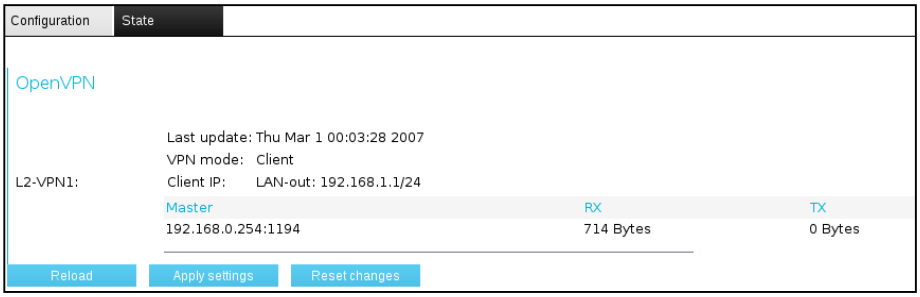
If a layer 3 connection is used, the "OpenVPN/DHCP" option must be configured for the L3 VPN interface in the same way:



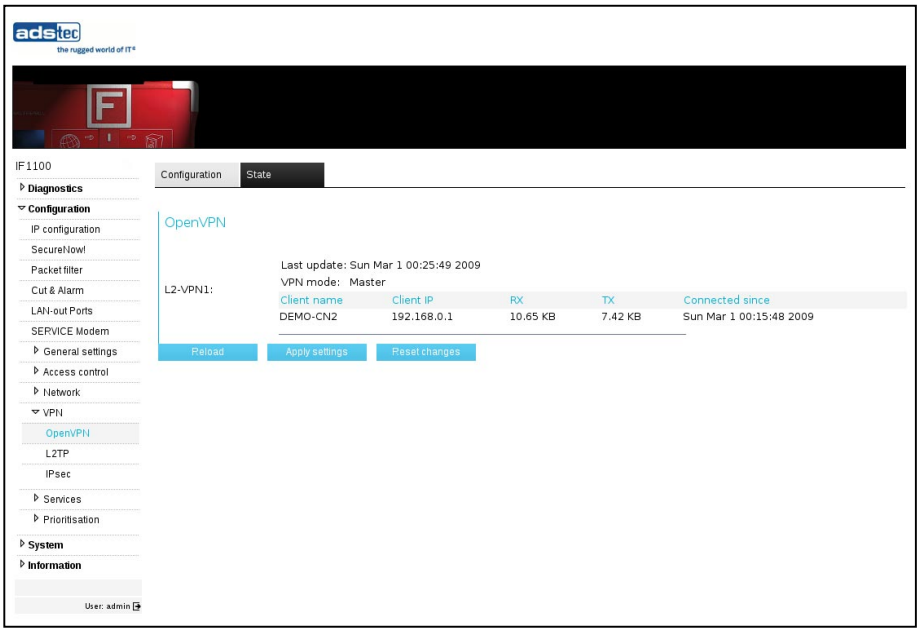
The option for static routes must be enabled, so that it matches the Server configuration ("Get static IP routes from OpenVPN Server"). Assigning the DNS server via OpenVPN is impossible.

OPENVPN STATUS

Once the OpenVPN configuration is completed, you can retrieve the status of connections in the status menu. For instance for the client:



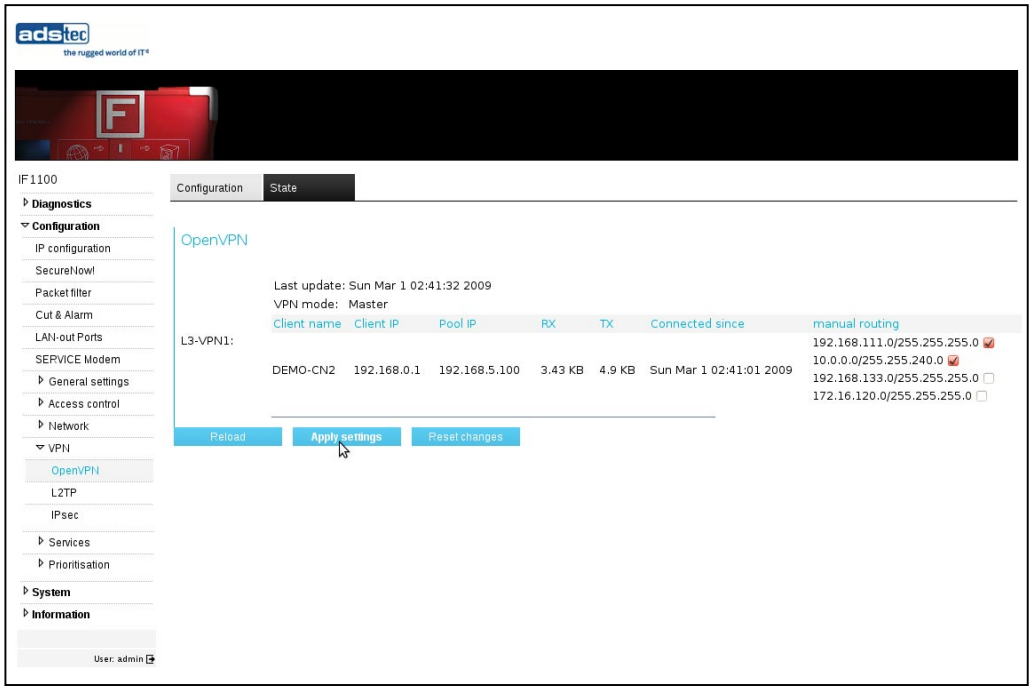
For instance for the server:



Additionally, the "OVPN" character sequence appears in the top right corner of the LC display, which indicates a currently running OpenVPN connection.

If OpenVPN Server and client both use the dynamic IP configuration with "OpenVPN/DHCP", additional information with respect to the IPs assigned from the address pool appears on the status page of the Server device. The ads-tec OpenVPN clients additionally transmit the local routing information of physical interfaces to the Server.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen



This routing information is shown in the "manual routing" column in the status view. Such a route can be selected and used for the running operation. This allows the Server device to reach other devices in subnets, which from the point of view of the Server are located behind the clients. This route is automatically removed once the client is disconnected. The corresponding setting can also not be saved, but will have to be reactivated after a restart of the Server device. Permanent routes can be created in the Configuration ☐ Network ☐ IP routing menu item.

EVENTLOG MESSAGES FOR OPENVPN

The following messages for OpenVPN may appear in the event log:

- *IF1xxx L2-VPN: 192.168.5.204:4420 [DEMO-CN5] Peer Connection Initiated with 192.168.5.204:4420*

(Indicates that the DEMO-CN5 client has successfully established a connection from source IP address 192.168.5.204 and TCP port 4420)

- *IF1xxx L2-VPN: TCP: connect to 192.168.5.204:1194 failed, will try again in 5 seconds: No route to host (errno=113)*

(Indicates a connection error of a client, which tries to connect to the server. In the example, no IP route exists for the server IP address.)

- *IF1xxx L2-VPN: VERIFY ERROR: depth=1, error=certificate is not yet valid: /C=DE/ST=Baden-Wuerttemberg/L=DEMO-LN/O=DEMO-ON/OU=DEMO-OUN/CN=DEMO-CN/emailAddress=democa@ads-tec.de*

(Error message telling that the used certificate is invalid, because the validity period does not match the system time.)

- Should the certificate be entered in a CRL and therefore be rejected by the remote device, no concrete error message will be displayed for this fact. An indication for this is

the fact, that the TCP connection is successfully established, but then immediately reset once the first data packet has been received. If in doubt, the log of the remote device should always be included in the investigation.

Additionally, comprehensive OpenVPN messages can be enabled by using the "Log Level" setting (in the Additional settings menu). This will give you support with any issues where the desired connections cannot be established.

INSTALLING OPENVPN UNDER WINDOWS

You'll find some notes on installation and application of OpenVPN under Windows on the website http://www.openvpn.net/index.php/open-source.html

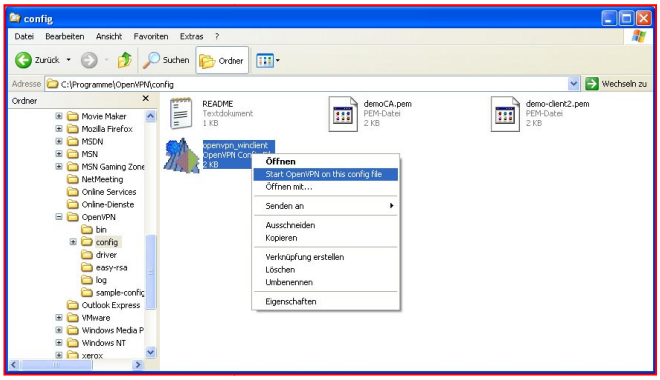
© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

CONFIGURATION AS AN OPENVPN CLIENT UNDER WINDOWS

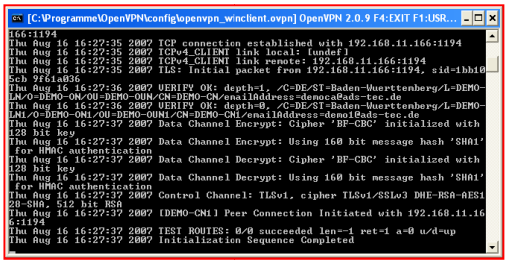
In order to configure an OpenVPN connection under Windows, a configuration file with an .ovpn file extension must be created in C:\Programmes\OpenVPN\config. The attached exemplary open_winclient.ovpn configuration may be used as a template for this.

The exemplary configuration connects the client with an OpenVPN server, which has the IP address 192.168.11.166 on port 1194 (this corresponds with the firewall from the "OpenVPN Server configuration" section), and uses the IP address 192.168.253.168 for the local TAP interface (OpenVPN tunnelling end point). The demo-client2.pem and demoCA.pem certificates required for authentication must also be copied to C:\Programmes\OpenVPN\config.

The OpenVPN connection is started by right-clicking on the file and selecting "Start OpenVPN on this config file".



This causes a prompt to open, in which you can watch the connection status. As soon as you close this prompt, the VPN connection will be terminated.


[C:\Programme\OpenVPN\config\openvpn_winclient.ovpn] OpenVPN 2.0.9 F4:EXIT F1:USR...
166:1194
Thu Aug 16 16:27:35 2007 TCP connection established with 192.168.11.166:1194
Thu Aug 16 16:27:35 2007 TCPv4_CLIENT link local: [undef]
Thu Aug 16 16:27:35 2007 TCPv4_CLIENT link remote: 192.168.11.166:1194
Thu Aug 16 16:27:35 2007 TLS: Initial packet from 192.168.11.166:1194, sid=1bb10
5cb 9f61a036
Thu Aug 16 16:27:36 2007 VERIFY OK: depth=1, /C=DE/ST=Baden-Wuerttenberg/L=DEMO-
LN/O=DEMO-ON/OU=DEMO-OUN/CN=DEMO-CN/emailAddress=democa@ads-tec.de
Thu Aug 16 16:27:36 2007 VERIFY OK: depth=0, /C=DE/ST=Baden-Wuerttenberg/L=DEMO-
LN1/O=DEMO-ON1/OU=DEMO-OUN1/CN=DEMO-CN1/emailAddress=demo1@ads-tec.de
Thu Aug 16 16:27:37 2007 Data Channel Encrypt: Cipher 'BF-CBC' initialized with
128 bit key
Thu Aug 16 16:27:37 2007 Data Channel Encrypt: Using 160 bit message hash 'SHA1'
for HMAC authentication
Thu Aug 16 16:27:37 2007 Data Channel Decrypt: Cipher 'BF-CBC' initialized with
128 bit key
Thu Aug 16 16:27:37 2007 Data Channel Decrypt: Using 160 bit message hash 'SHA1'
for HMAC authentication
Thu Aug 16 16:27:37 2007 Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-AES1
28-SHA, 512 bit RSA
Thu Aug 16 16:27:37 2007 [DEMO-CN1] Peer Connection Initiated with 192.168.11.16
6:1194
Thu Aug 16 16:27:37 2007 TEST ROUTES: 0/0 succeeded len=-1 ret=1 a=0 u/d-up
Thu Aug 16 16:27:37 2007 Initialization Sequence Completed

Note:

The system time on the VPN Server and client must match the time specified in the certificates, or they will be invalid if the system time is outside the validity period!
Instead of using the "ifconfig..." OpenVPN config line, you could also manually assign the IP address to the TAP adapter under Control panel/Network connections (the "ifconfig..." line must be separated by a semicolon in order to mark it as a comment, in that case).
If a proxy server is used, the server access data may be set in the "http-proxy" config line (the semicolon must be removed, since this line would be considered a comment, otherwise). If user name and password are required, they must be stored in a separate file.
The certificates may also be stored at a central location (e.g. at C:\Certificates). The complete path information must be specified for the ca, cert and key entries, in that case (e.g. ca C:\\ Certificates\\demoCA.pem). Warning: The backslashes must be doubles!
A detailed explanation of all options can be found at http://openvpn.net/
From OpenVPN version 2.0.9, the required routing information is automatically entered. With older versions, a route must manually be added by using the route command, in order to route the traffic for the subnet via the local TAP adapter of the client. If the client is, for instance, using 192.168.1.168 as an IP address for the TAP adapter, the traffic for 192.168.1.0/24 must be routed via 192.168.1.168. This happens in the open command prompt: route add 192.168.1.0 mask 255.255.255.0 192.168.1.168

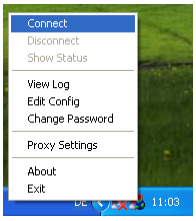
© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

Using the OpenVPN GUI

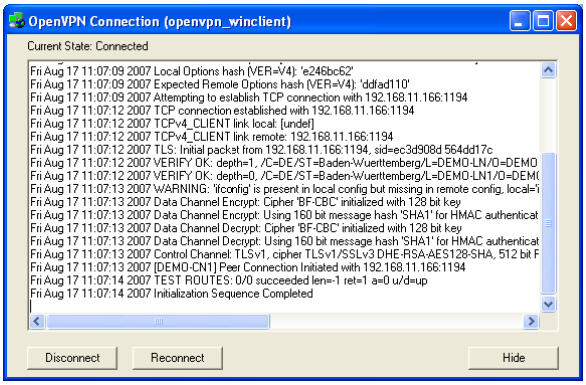
OpenVPN GUI is an additional tool for OpenVPN, and is available at http://openvpn.se/ . The GUI tool is very handy for enabling and monitoring OpenVPN connections. If the tool is started, a corresponding icon (a network icon including red monitor screens, if there is no active connection) will appear in the info area (on the bottom right in the screen):



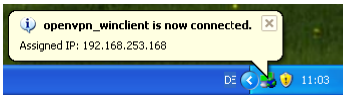
By right-clicking on this icon, a menu will appear, which allows changing the configuration and enabling the connection.



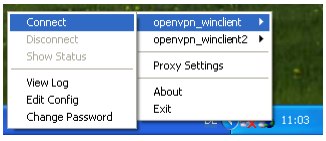
Corresponding messages are displayed in a status window, if a connection is established.


OpenVPN Connection (openvpn_winclient)
Current State: Connected
Fri Aug 17 11:07:09 2007 Local Options hash (VER=V4): 'e246bc62'
Fri Aug 17 11:07:09 2007 Expected Remote Options hash (VER=V4): 'ddfad110'
Fri Aug 17 11:07:09 2007 Attempting to establish TCP connection with 192.168.11.166:1194
Fri Aug 17 11:07:12 2007 TCP connection established with 192.168.11.166:1194
Fri Aug 17 11:07:12 2007 TCPv4_CLIENT link local: [undef]
Fri Aug 17 11:07:12 2007 TCPv4_CLIENT link remote: 192.168.11.166:1194
Fri Aug 17 11:07:12 2007 TLS: Initial packet from 192.168.11.166:1194, sid=ec3d908d 564dd17c
Fri Aug 17 11:07:12 2007 VERIFY OK: depth=1, /C=DE/ST=Baden-Wuerttemberg/L=DEMO-LN/O=DEMO
Fri Aug 17 11:07:12 2007 VERIFY OK: depth=0, /C=DE/ST=Baden-Wuerttemberg/L=DEMO-LN1/O=DEM(
Fri Aug 17 11:07:13 2007 WARNING: 'ifconfig' is present in local config but missing in remote config, local='i
Fri Aug 17 11:07:13 2007 Data Channel Encrypt: Cipher 'BF-CBC' initialized with 128 bit key
Fri Aug 17 11:07:13 2007 Data Channel Encrypt: Using 160 bit message hash 'SHA1' for HMAC authenticat
Fri Aug 17 11:07:13 2007 Data Channel Decrypt: Cipher 'BF-CBC' initialized with 128 bit key
Fri Aug 17 11:07:13 2007 Data Channel Decrypt: Using 160 bit message hash 'SHA1' for HMAC authenticat
Fri Aug 17 11:07:13 2007 Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-AES128-SHA, 512 bit F
Fri Aug 17 11:07:13 2007 [DEMO-CN1] Peer Connection Initiated with 192.168.11.166:1194
Fri Aug 17 11:07:14 2007 TEST ROUTES: 0/0 succeeded len=-1 ret=1 a=0 u/d=up
Fri Aug 17 11:07:14 2007 Initialization Sequence Completed
Disconnect
Reconnect
Hide

The window is closed as soon as the connection is established (but may be displayed again by using the "Show status" button in the GUI menu), and a message appears in the info area.



One sub-item per connection will appear in the GUI menu next to "Connect" if several OpenVPN connections have been defined.



Note:

Proxy settings may be made regardless of the configuration file by using the "Proxy settings" menu item (e.g. adopting the Internet Explorer settings). If several OpenVPN connections exist, active connections will be ticked in the box in front of their menu item.

11.3 OpenVPN server under Windows

General

This use case describes the configuration of several OpenVPN servers under Windows. By using OpenVPN, you can exchange data via a complex transmission network like inside a (virtual) internal LAN. In order to do so, the subnets defining the virtual LAN are connected by an Open VPN tunnel between an OpenVPN server (Server) and an OpenVPN client.

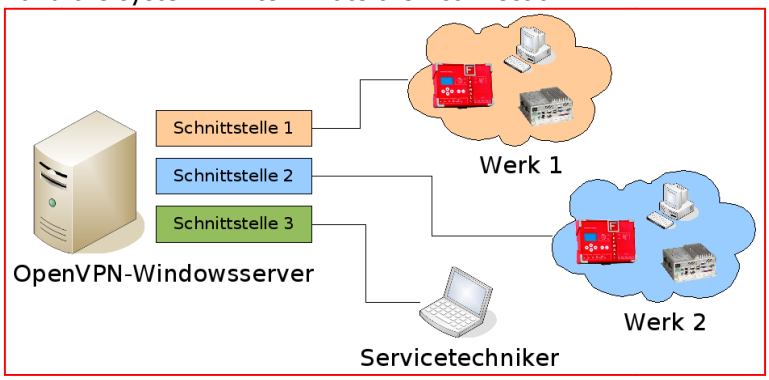
Note:

Please refer to the "OpenVPN" use case for configuration as an OpenVPN client and for configuring the IF1000.

Remote maintenance scenario

Remote maintenance by using a centralised server is a popular application. In the event of a service case, the system to be maintained connects with one of the OpenVPN server endpoints and the technician with another one.

So, you can, for instance assign a dedicated server endpoint to each customer, and define another one for the technicians. The technician will then be able to communicate with the customer network via corresponding routing and filter settings, but the customer networks cannot communicate with each other. As soon as the servicing has been completed, both the technician and the system will terminate their connection.



Note:

Exemplary certificates based on the demoCA.pem example CA are used. For a real application, you'll have to generate your own certificates, since the demo certificates are freely available and thus are not safe to use. See therefore the "Certificates" use case.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

INSTALLING OPENVPN

You'll find notes on the installation and application of OpenVPN at http://openvpn.net/INSTALL-win32.html. Generally you'll need the following software:

- OpenSSL (http://www.openssl.org/related/binaries.html)
- OpenVPN (http://openvpn.net/download.html)

First, you'll have to unpack and install the OpenSSL archive, and then the OpenVPN archive, by double-clicking on it.

Note:

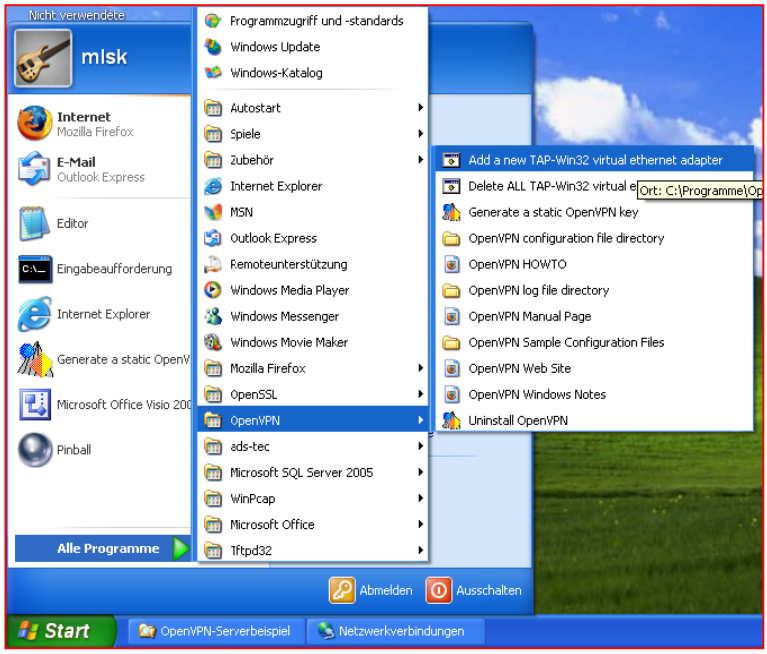
With OpenVPN, a warning that the software does not run because of a missing Microsoft test may occur. This warning can be ignored and you can continue with the installation.

In order to use OpenVPN, you need to have administrator rights.

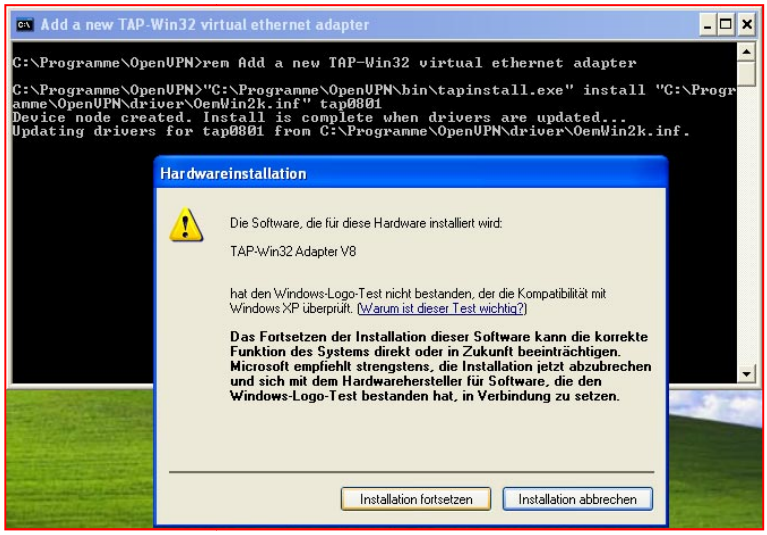
The regular installation path for OpenVPN is C:\Programmes\OpenVPN. If this path has been changed, the paths mentioned further below must be adapted accordingly.

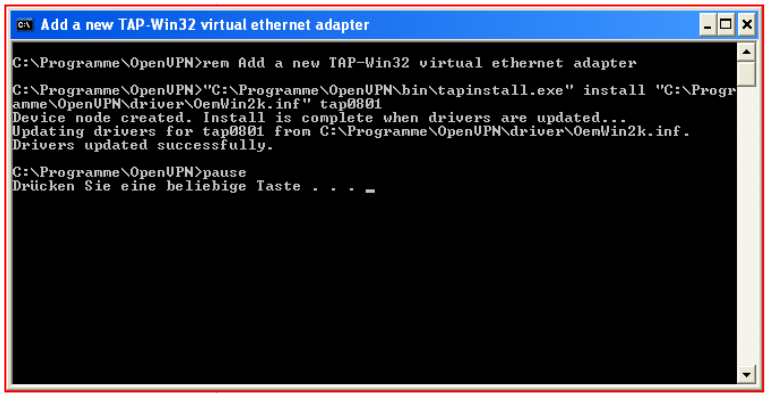
CREATING THE OPENVPN INTERFACES

First you'll have to add the desired number of OpenVPN interfaces (TAP adapters) by using the OpenVPN menu. Each time you use "Add a new TAP-Win32 virtual Ethernet adapter", a new interface is created.

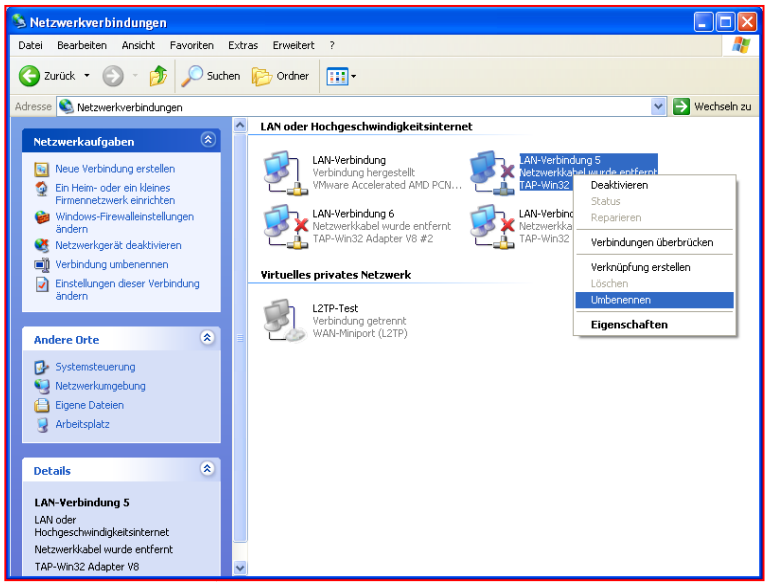


Under certain circumstances, an error message might occur several times during the installation. However, you can continue the process and ignore the message.


Add a new TAP-Win32 virtual ethernet adapter
C:\Programme\OpenVPN>rem Add a new TAP-Win32 virtual ethernet adapter
C:\Programme\OpenVPN>"C:\Programme\OpenVPN\bin\tapinstall.exe" install "C:\Programme\OpenVPN\driver\OemWin2k.inf" tap0801
Device node created. Install is complete when drivers are updated...
Updating drivers for tap0801 from C:\Programme\OpenVPN\driver\OemWin2k.inf.
Hardwareinstallation
Die Software, die für diese Hardware installiert wird:
TAP-Win32 Adapter V8
hat den Windows-Logo-Test nicht bestanden, der die Kompatibilität mit Windows XP überprüft. (Warum ist dieser Test wichtig?)
Das Fortsetzen der Installation dieser Software kann die korrekte Funktion des Systems direkt oder in Zukunft beeinträchtigen. Microsoft empfiehlt strengstens, die Installation jetzt abzubrechen und sich mit dem Hardwarehersteller für Software, die den Windows-Logo-Test bestanden hat, in Verbindung zu setzen.
Installation fortsetzen
Installation abbrechen

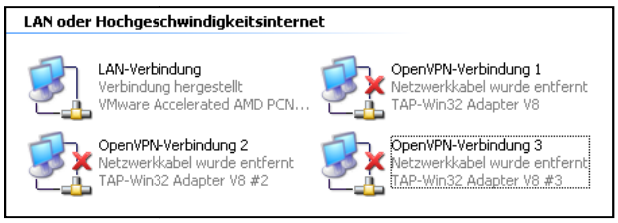

Add a new TAP-Win32 virtual ethernet adapter
C:\Programme\OpenVPN>rem Add a new TAP-Win32 virtual ethernet adapter
C:\Programme\OpenVPN>"C:\Programme\OpenVPN\bin\tapinstall.exe" install "C:\Programme\OpenVPN\driver\OemWin2k.inf" tap0801
Device node created. Install is complete when drivers are updated...
Updating drivers for tap0801 from C:\Programme\OpenVPN\driver\OemWin2k.inf.
Drivers updated successfully.
C:\Programme\OpenVPN>pause
Drücken Sie eine beliebige Taste . . .

Subsequently, these new interfaces must be renamed in the network connections panel.



An OpenVPN configuration will identify related interfaces by their names. For our example, we simply use the designations "OpenVPN connection 1", "OpenVPN connection 2", etc.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen



An OpenVPN configuration will identify related interfaces by their names. For our example, we simply use the designations OpenVPN connection 1, OpenVPN connection 2, etc.

Note:

Any number of clients might connect on a server connection, as long as the authentication process is successful. This means that an endpoint does not have to be defined for every connection. The division into customers and groups of technicians, for instance, might be useful.

CONFIGURING AN OPENVPN CONNECTION AS A SERVER

port 443

proto tcp

dev tap

dev-node "OpenVPN connection 1"

ca demoCA.pem

cert demo-server1.pem

key demo-server1.pem

dh dh1024.pem

server 192.168.10.0 255.255.255.0

ifconfig-pool-persist ipp.txt

keepalive 10 120

persist-key

persist-tun

status openvpn-status-server1.log

verb 3

In order to configure an OpenVPN connection under Windows, a corresponding configuration file with an .ovpn file extension must be created in C:\Programmes\OpenVPN\config. The configuration for ads-tec-if-server1.ovpn, for the first exemplary connection, is for instance as follows:

The Windows server will authenticate itself for this connection by using the demo-server1.pem certificate (which also includes the required private key), and will in turn accept all clients, which have a certificate signed by demoCA.pem. IP addresses from the 192.168.10.0/24 subnet range will be assigned, while the server itself is generally always using the first IP address from this range. In this case that is 192.168.10.1. The certificates don't have any path specification but must also be located in C:\Programmes\OpenVPN\config. As an alternative, the complete path information might

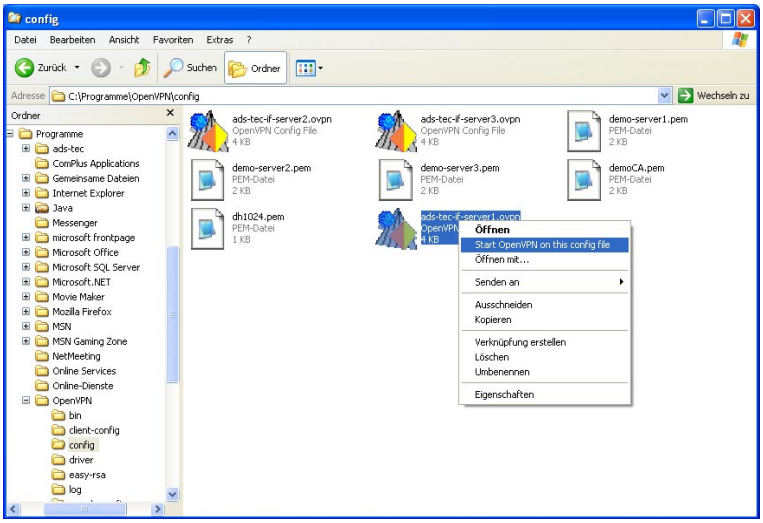
be given in every case, where a centralised folder is used for certificates (for instance C:\\Certificates; Warning: The backslashes must be doubles!).

Note:

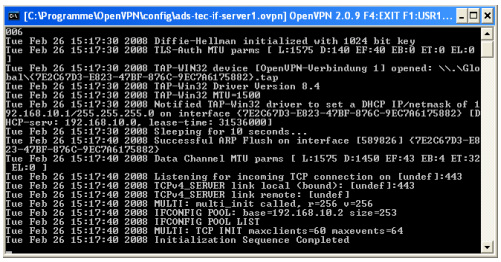
- *Configuration files exist as an attachment and include detailed comments on individual options.*
- *Every server connection requires an unambiguous port. The first connection is using port 443, which is usually dedicated for HTTPS. Because of this, the remote terminal can simply run through a proxy without having to configure the proxy specifically.*
- *Both other exemplary connections, the ads-tec-if-server2.ovpn and ads-tec-if-server3.ovpn connection, are designed in the same way. The second one is using the 192.168.20.0/24 subnet and port 1194. The third one is using the 192.168.30.0/24 subnet and port 1195.*
- *The ads-tec-if-server3.ovpn configuration shows a particularity. The push "route ..." command is used there, in order to automatically specify the routes for the other networks to the client. This allows the service technician to reach them without having to make a local configuration. The certificates and the dh1024.pem file are also included in the attachment.*

STARTING AN OPENVPN CONNECTION

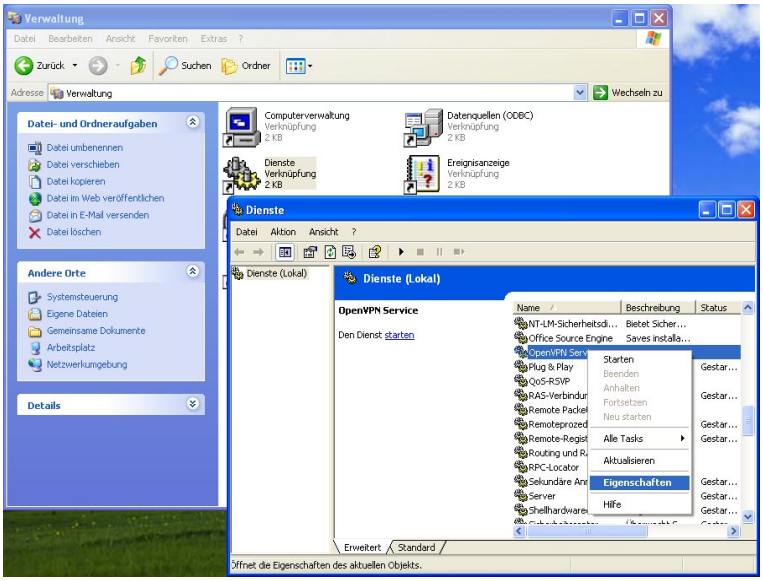
The OpenVPN connection is started by right-clicking on the file and selecting "Start OpenVPN on this config file".



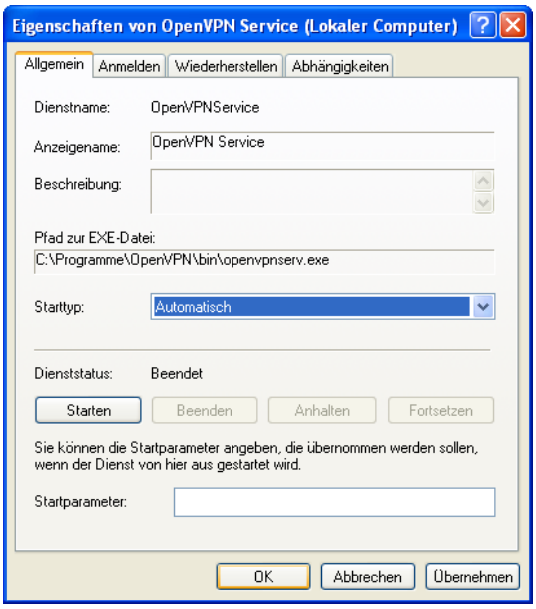
This causes a prompt to open, in which you can watch the connection status. As soon as you close this prompt, the OpenVPN connection will be terminated.


[C:\Programme\OpenVPN\config\ads-tec-if-server1.ovpn] OpenVPN 2.0.9 F4:EXIT F1:USR1...
006
Tue Feb 26 15:17:30 2008 Diffie-Hellman initialized with 1024 bit key
Tue Feb 26 15:17:30 2008 TLS-Auth MTU parms [L:1575 D:140 EF:40 EB:0 ET:0 EL:0
]
Tue Feb 26 15:17:30 2008 TAP-WIN32 device [OpenVPN-Verbindung 1] opened: \\.\Glo
bal\{7E2C67D3-E823-47BF-876C-9EC7A6175082}.tap
Tue Feb 26 15:17:30 2008 TAP-Win32 Driver Version 8.4
Tue Feb 26 15:17:30 2008 TAP-Win32 MTU=1500
Tue Feb 26 15:17:30 2008 Notified TAP-Win32 driver to set a DHCP IP/netmask of 1
92.168.10.1/255.255.255.0 on interface {7E2C67D3-E823-47BF-876C-9EC7A6175082} [D
HCP-serv: 192.168.10.0, lease-time: 31536000]
Tue Feb 26 15:17:30 2008 Sleeping for 10 seconds...
Tue Feb 26 15:17:40 2008 Successful ARP Flush on interface [589826] {7E2C67D3-E8
23-47BF-876C-9EC7A6175082}
Tue Feb 26 15:17:40 2008 Data Channel MTU parms [L:1575 D:1450 EF:43 EB:4 ET:32
EL:0]
Tue Feb 26 15:17:40 2008 Listening for incoming TCP connection on [undef]:443
Tue Feb 26 15:17:40 2008 TCPv4_SERVER link local (bound): [undef]:443
Tue Feb 26 15:17:40 2008 TCPv4_SERVER link remote: [undef]
Tue Feb 26 15:17:40 2008 MULTI: multi_init called, r=256 v=256
Tue Feb 26 15:17:40 2008 IFCONFIG POOL: base=192.168.10.2 size=253
Tue Feb 26 15:17:40 2008 IFCONFIG POOL LIST
Tue Feb 26 15:17:40 2008 MULTI: TCP INIT maxclients=60 maxevents=64
Tue Feb 26 15:17:40 2008 Initialization Sequence Completed

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

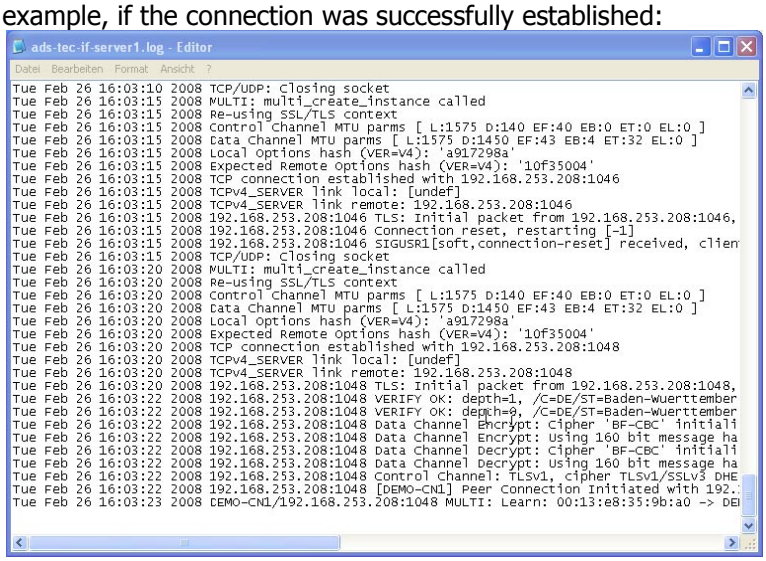


OpenVPN can be configured in the Control panel under Administrative tools/Services in such way, that all connections defined in C:\Programmes\OpenVPN\config are directly enabled when the computer is started up. In order to do so, right-click on OpenVPN service, and set the Startup type under Properties to Automatic.



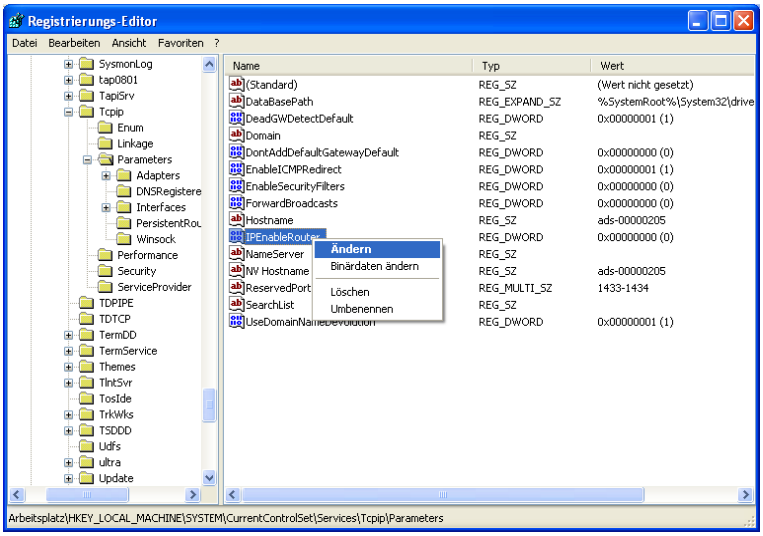
STATUS OF AN OPENVPN CONNECTION

By using the status command in the configuration, you can define a log file, which is updated once per minute, and in which you can read the current status of the connection. The log files are located in C:\Programmes\OpenVPN\log, and could look like this, for example, if the connection was successfully established:


ads-tec-if-server1.log - Editor
Datei Bearbeiten Format Ansicht ?
Tue Feb 26 16:03:10 2008 TCP/UDP: Closing socket
Tue Feb 26 16:03:15 2008 MULTI: multi_create_instance called
Tue Feb 26 16:03:15 2008 Re-using SSL/TLS context
Tue Feb 26 16:03:15 2008 Control Channel MTU parms [L:1575 D:140 EF:40 EB:0 ET:0 EL:0]
Tue Feb 26 16:03:15 2008 Data Channel MTU parms [L:1575 D:1450 EF:43 EB:4 ET:32 EL:0]
Tue Feb 26 16:03:15 2008 Local Options hash (VER=V4): 'a917298a'
Tue Feb 26 16:03:15 2008 Expected Remote Options hash (VER=V4): '10f35004'
Tue Feb 26 16:03:15 2008 TCP connection established with 192.168.253.208:1046
Tue Feb 26 16:03:15 2008 TCPv4_SERVER link local: [undef]
Tue Feb 26 16:03:15 2008 TCPv4_SERVER link remote: 192.168.253.208:1046
Tue Feb 26 16:03:15 2008 192.168.253.208:1046 TLS: Initial packet from 192.168.253.208:1046,
Tue Feb 26 16:03:15 2008 192.168.253.208:1046 Connection reset, restarting [-1]
Tue Feb 26 16:03:15 2008 192.168.253.208:1046 SIGUSR1[soft,connection-reset] received, clien
Tue Feb 26 16:03:15 2008 TCP/UDP: Closing socket
Tue Feb 26 16:03:20 2008 MULTI: multi_create_instance called
Tue Feb 26 16:03:20 2008 Re-using SSL/TLS context
Tue Feb 26 16:03:20 2008 Control Channel MTU parms [L:1575 D:140 EF:40 EB:0 ET:0 EL:0]
Tue Feb 26 16:03:20 2008 Data Channel MTU parms [L:1575 D:1450 EF:43 EB:4 ET:32 EL:0]
Tue Feb 26 16:03:20 2008 Local Options hash (VER=V4): 'a917298a'
Tue Feb 26 16:03:20 2008 Expected Remote Options hash (VER=V4): '10f35004'
Tue Feb 26 16:03:20 2008 TCP connection established with 192.168.253.208:1048
Tue Feb 26 16:03:20 2008 TCPv4_SERVER link local: [undef]
Tue Feb 26 16:03:20 2008 TCPv4_SERVER link remote: 192.168.253.208:1048
Tue Feb 26 16:03:20 2008 192.168.253.208:1048 TLS: Initial packet from 192.168.253.208:1048,
Tue Feb 26 16:03:22 2008 192.168.253.208:1048 VERIFY OK: depth=1, /C=DE/ST=Baden-Wuerttember
Tue Feb 26 16:03:22 2008 192.168.253.208:1048 VERIFY OK: depth=0, /C=DE/ST=Baden-Wuerttember
Tue Feb 26 16:03:22 2008 192.168.253.208:1048 Data Channel Encrypt: Cipher 'BF-CBC' initiali
Tue Feb 26 16:03:22 2008 192.168.253.208:1048 Data Channel Encrypt: Using 160 bit message ha
Tue Feb 26 16:03:22 2008 192.168.253.208:1048 Data Channel Decrypt: Cipher 'BF-CBC' initiali
Tue Feb 26 16:03:22 2008 192.168.253.208:1048 Data Channel Decrypt: Using 160 bit message ha
Tue Feb 26 16:03:22 2008 192.168.253.208:1048 Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE
Tue Feb 26 16:03:22 2008 192.168.253.208:1048 [DEMO-CN1] Peer Connection Initiated with 192.
Tue Feb 26 16:03:23 2008 DEMO-CN1/192.168.253.208:1048 MULTI: Learn: 00:13:e8:35:9b:a0 -> DE

ENABLING IP FORWARDING

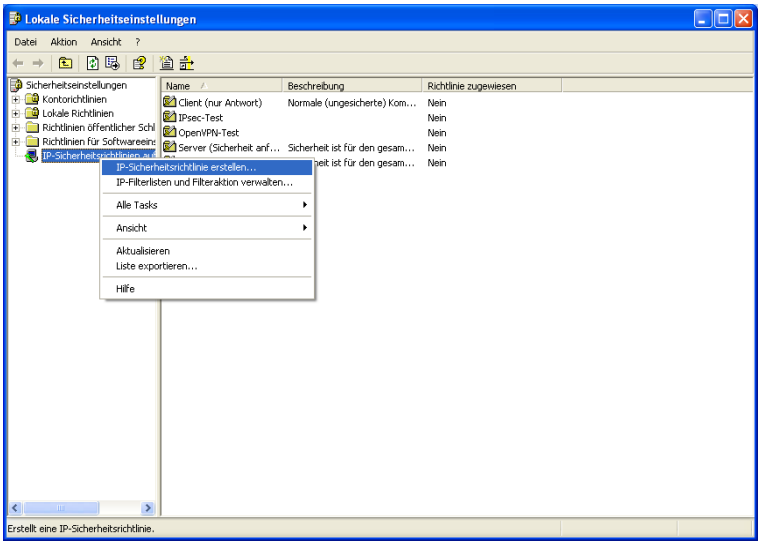
In order to allow different OpenVPN interfaces to communicate with each other, IP forwarding must be enabled. You can check this by using the registry editor. In order to do so, enter the regedit command under Start/Run... and verify the value of IPEnableRouter under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters. Should this value not be set to 1, the value can be adapted by right-clicking on the variable in the Modify menu item.



© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

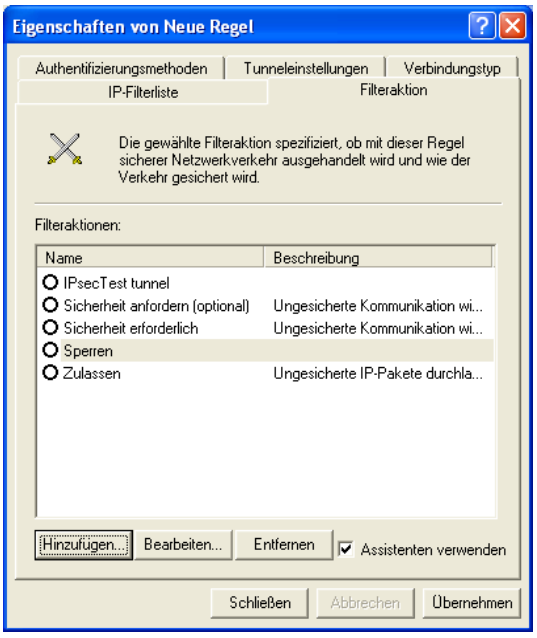
IP FILTERING BETWEEN OPENVPN INTERFACES

In order to bar data traffic between different factories (so that only technicians can gain access), a corresponding IP security policy must be created. By using Start/Run... and entering the secpol.msc command, you can start the local security policy snap-in in the Microsoft Management Console. This wizard is started by right-clicking on IP security policies on Local computer, and by clicking there on "Create IP security policy...".



"OpenVPN-Server" must be entered there as the name. The default response rule must *not* be activated, but the "Edit properties" checkbox must be checked. Finally click on "Finish".

Then untick the "Use wizard" option and click on "Add". Switch to the "Filter action" tab, enable the Wizard here and click on "Add". Then use "Bar" as the name for this rule, set "Bar" as a general option, and complete the process with "Finish". Should "Allow" as the opposite action not yet exist, it must be created in the same way, but this time by using "Allow" as the name, and with the "Allow" option enabled.

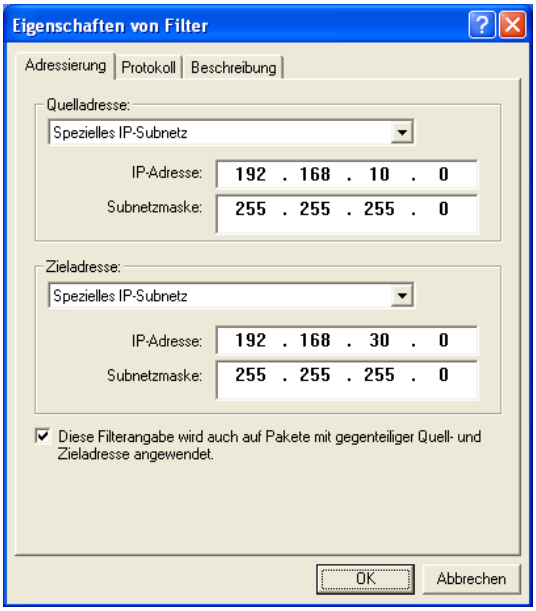


Subsequently go back to the IP filter list tab and click on Add in this tab. Subsequently go back to the "IP filter list" tab and click on "Add" in this tab. Two filter lists are required for

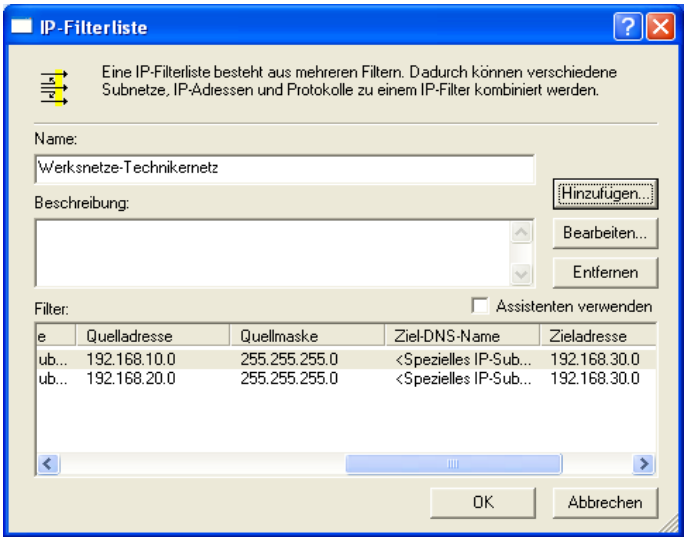
allowing the traffic between an individual company and the subnet of the technician, and to bar the remaining traffic between the individual factories.

You can enter "Factory networks - Technician network" as the name for the first list, for example. Then, one filter for each factory, which includes the traffic between the factory subnet network and the technician network, must be created. In order to do so, you'll have to disable the wizard and then click on "Add".

Select "Specific IP subnet" in the Source and destination address line, specify the factory subnet as the Source address (e.g. 192.168.10.0 with 255.255.255.0), and the subnet of the technicians as the Destination address (e.g. 192.168.30.0 with 255.255.255.0). The option "This filter specification is also applied to packets with different source and destination address." must remain selected.

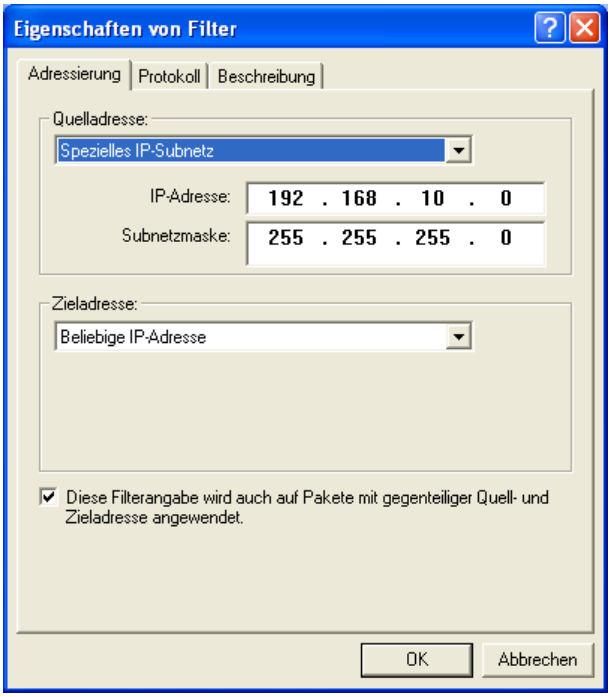


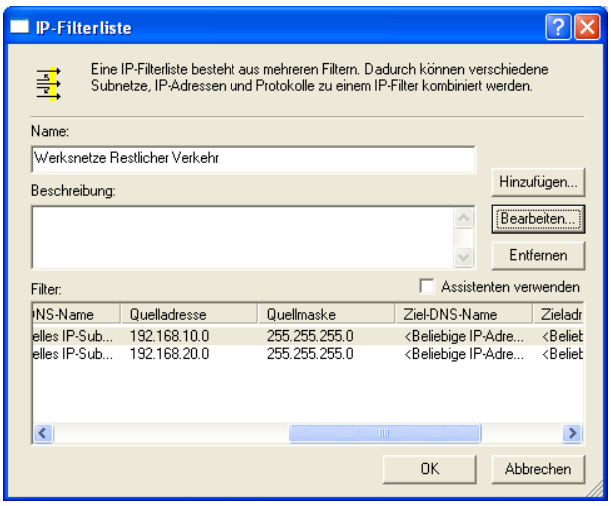
In the remote maintenance example, a filter for the subnet of the second factory (192.168.20.0/24) must be added in the same way, so that this filter list will contain two filters.



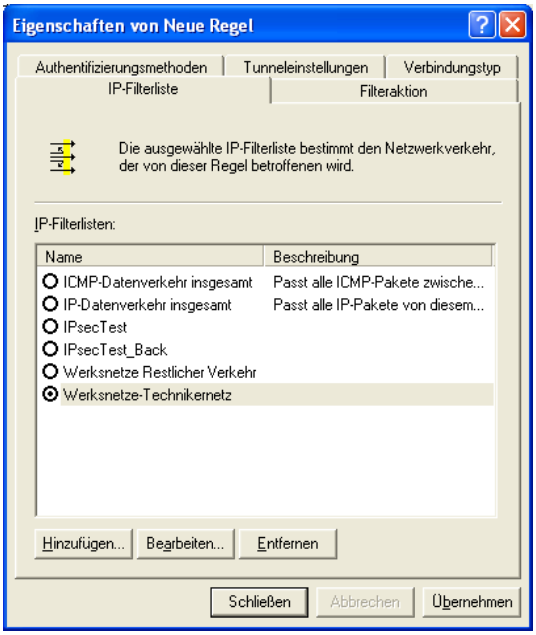
"Factory networks - residual traffic" might be used as a name for the second list. This list is structured in the same way (one filter required for each factory), but the destination address is set to "Any IP address".

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

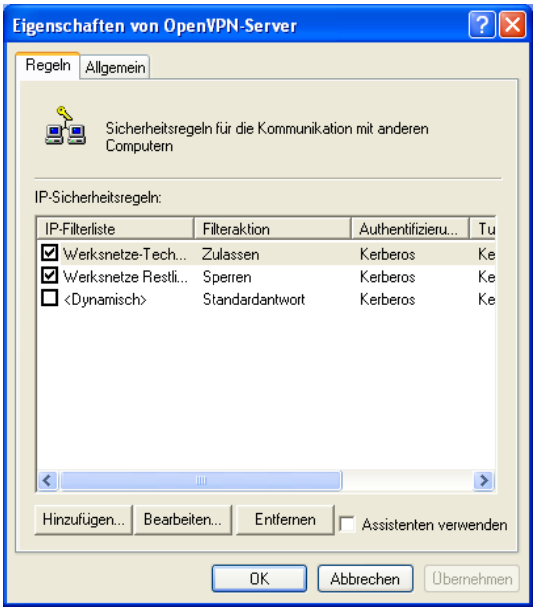




This has the results that two new filter lists exist.

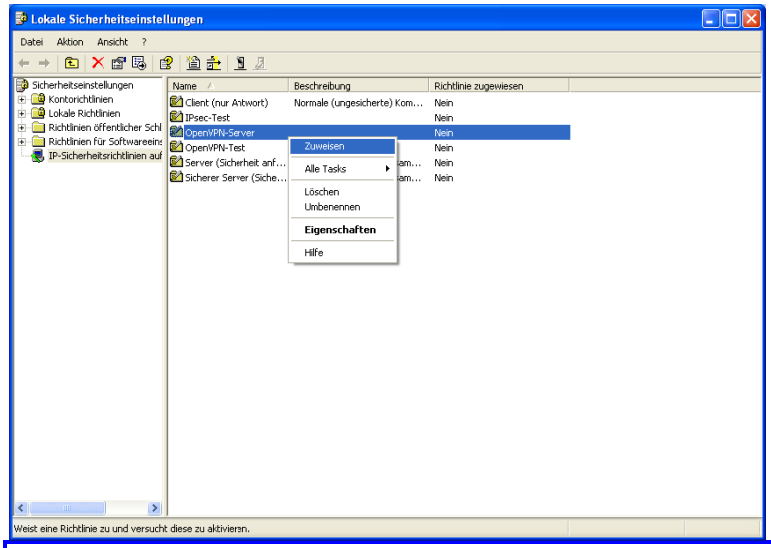


In the final step, you have to select the "Allow" filter action, push the "Store" and then the "OK" button for the "Factory networks - technician network" IP-filter list. Push the "Add" button in the Policy one more time and associate "Factory networks - residual traffic" with "Bar" in the same way. As a result, the completed policy now includes two rules, one of which bars any traffic from the OpenVPN connections, whereas the other one allows the traffic into the technician subnet as an exception.



The security policy must finally be assigned in order to become active.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

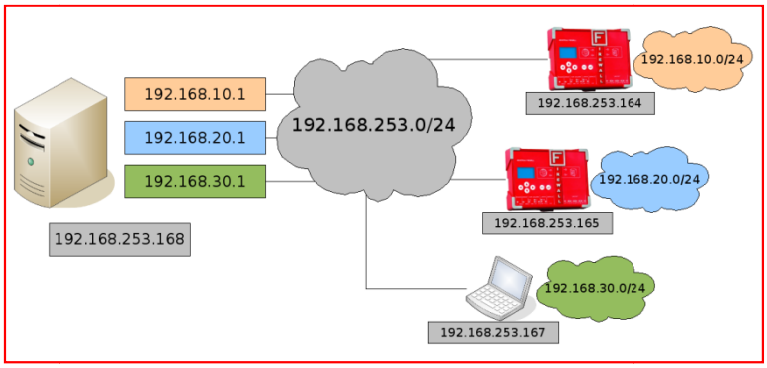


Note:

If the default firewall of Windows is active, the access to the ports for OpenVPN connections must be enabled, so that the clients can be connected.

CONFIGURING THE IF1000 AS AN OPENVPN CLIENT

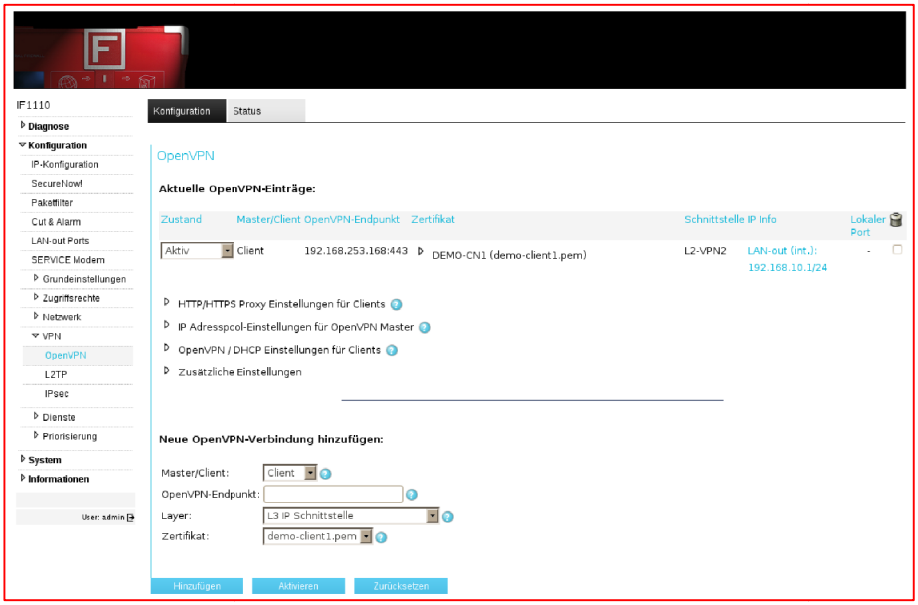
On an IF1000 series device, you just have to define a client OpenVPN connection with the Windows server, and to create the route for the technician network. Let's assume, for instance, that the Windows server, the two factory firewalls and the technician laptop are connected via the 192.168.253.0/24 subnet according to the remote maintenance scenario, and that the Windows server has the IP address 192.168.253.168.



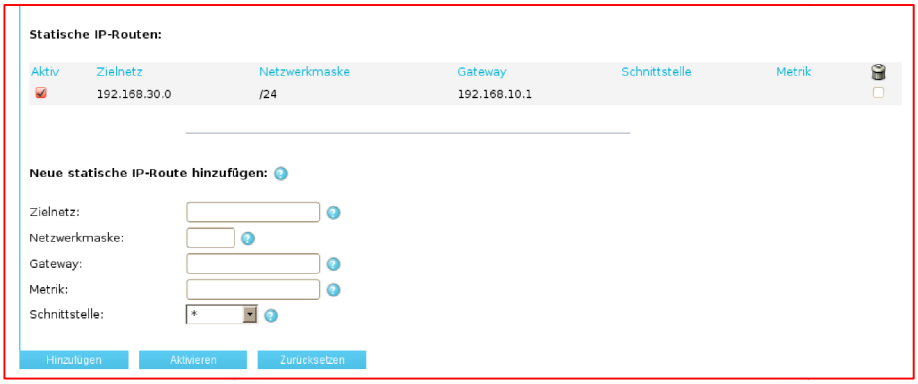
On the first firewall (on the one that runs in routing mode and is connected with the 192.168.10.0/24 subnet via the LAN-out interface), you'll have to create an OpenVPN entry with 192.168.253.168:443 as the destination address (according to the port specification from the configuration file), and to use one of the demo certificates for it (e.g. demo-client1.pem).

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

Additionally, the OpenVPN connection of the Windows server (192.168.10.1) must be entered as the gateway for the technician network (192.168.30.0/24 in this example).



In the same way, you'll have to create an OpenVPN entry using the 192.168.253.168:1194 endpoint and the demo-client3.pem certificate on the second firewall, which is connected with the 192.168.20.0/24 subnet. The 192.168.20.1 IP address must be entered as a gateway for the 192.168.30.0/24 subnet.



Note:

The first IP address from the subnet address range must never be used in the firewalls LAN-Out subnet (e.g. the 192.168.10.1 address), because it will always be used by the server.

The route towards the relevant technician subnet must always be entered in the firewall, in order to allow both OpenVPN networks to communicate.

You'll find the exemplary firewall configurations in the attachment. "factory1.cfg" is the configuration of factory 1, and "factory2.cfg" is the configuration of factory 2.

CONFIGURING AN OPENVPN CLIENT UNDER WINDOWS

First, OpenVPN must be installed on the computer (e.g. on the service technician's laptop) according to above description. The automatically created TAP interface must be configured as "Automatically refer to IP address". You can check this in the Network connections by right-clicking on the TAP interface and verifying the settings under Properties/Internet protocol (TCP/IP).

The configuration and related certificates must also be created or stored at C:\Programmes\OpenVPN\config, according to above example. In this case, this refers to the attached "technician.ovpn" file and the demoCA.pem, as well as to the demo-client2.pem certificate.

If the connection is manually established by right-clicking on the configuration file, the technicians can remotely maintain the machines to which they have dialled in without having to make any further settings.



Note:

You'll find a detailed explanation concerning the client configuration in the "OpenVPN" use case.

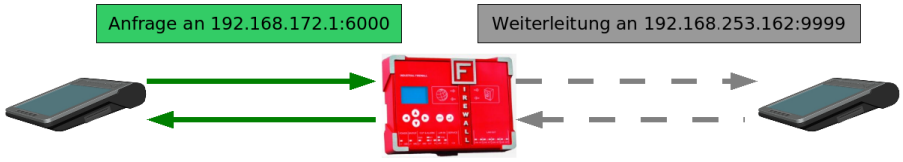
© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

11.4 PORT FORWARDING

GENERAL

Port forwarding allows the forwarding of connections to a subscriber in a second network via freely selectable ports. For the person with the external access it then looks, as if the service would be provided by the firewall, although it actually originates from a computer in the LAN beyond the firewall. In this way, a computer can e.g. act as a server in the Internet, although it cannot directly be accessed (e.g. due to NAT masquerading).

As an example of application, the firewall should here provide a TCP based service on port 6000 to the outside (LAN-in), which is in fact provided by a computer of the LAN behind the firewall (LAN-out) with IP address 192.168.1.100 on port 9999. The Firewall should in the example use the IP address 192.168.0.1 for LAN-in and the IP address 192.168.1.1 for LAN-out.

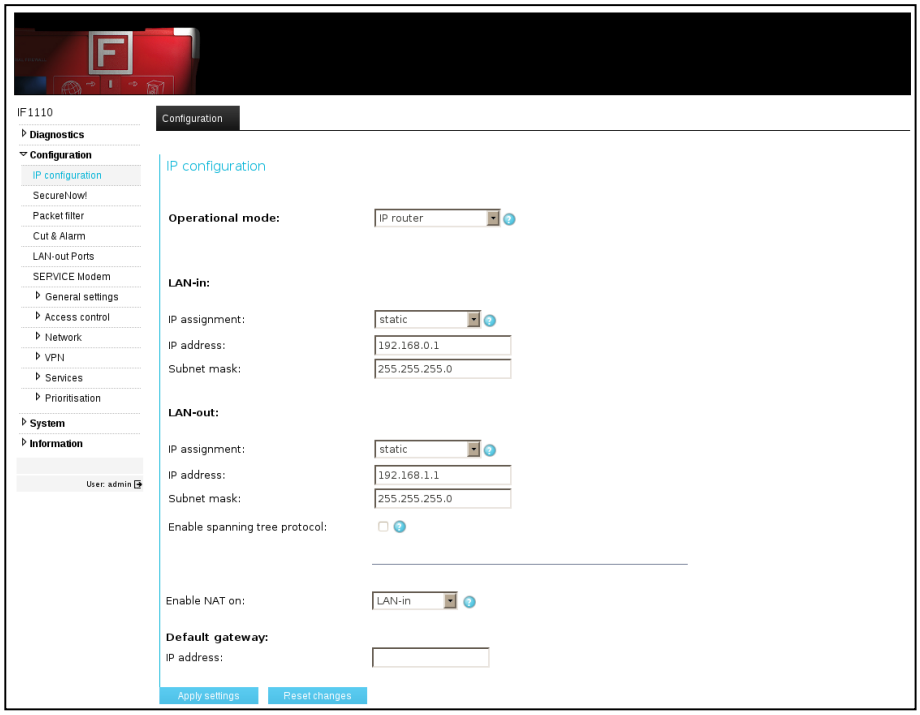


ENABLING NAT MASQUERADING

If port forwarding should be usable at all, the firewall must be allowed to change the IP addresses of incoming and outgoing packets, in order to make the service, which is actually located in the internal LAN, transparent to the outside world and accessible via the firewall. The option "Enable NAT" must be set to "LAN-in" on the "Configuration ☐ IP configuration" page, in order to realise this.

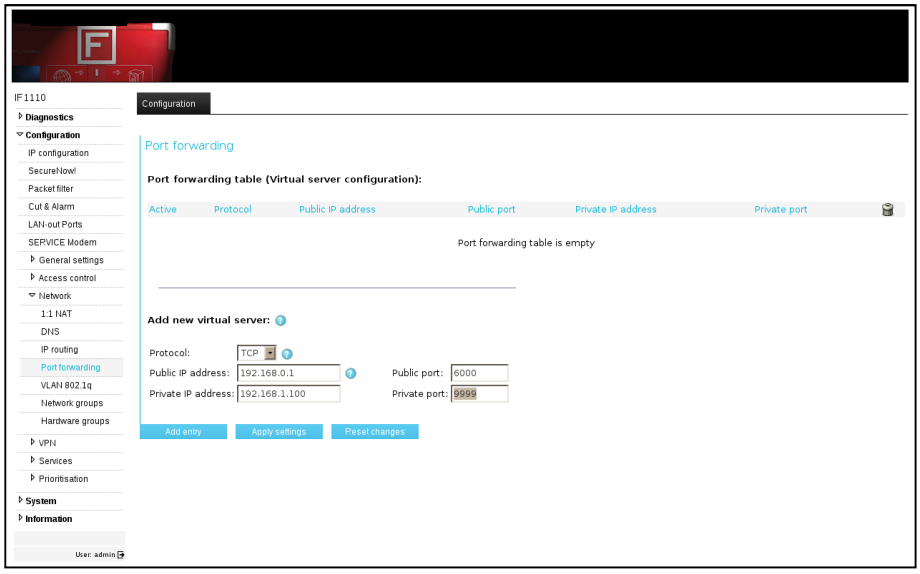
Note:

The firewall must either run in IP router or IP router extended mode for NAT to be usable.



ADDING A PORT FORWARDING ENTRY

Port forwarding entries can be defined in the "Configuration ☐ Network ☐ Port forwarding" menu item. This requires that the "Public port" (via which the service can be addresses on the firewall), the "Private port" (the actual port, on which the service runs on the local host computer), the transmission "Protocol" and the "IP address" of the local host computer are specified. This entry is created with "Add entry".



The service can then be addressed from the outside by using 192.168.0.1:6000, although it actually (but not visibly from the outside) runs on the host with IP 192.168.1.100:9999.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

DELETING PORT FORWARDING ENTRIES

If you'd like to delete a definition, you'll have to check the checkbox underneath the trash can icon for the corresponding entry, and then select “Active”.



ENABLING/DISABLING OF PORT FORWARDING ENTRIES

Port forwarding entries can temporarily be disabled by clicking on the corresponding checkbox in the "Active" column in order to untick it (disable it), and then push "Apply settings". The definition then remains existent, and can be re-enabled at any point in time.

RELEASING A FORWARDED PORT

The device default setting allows all packets on layer 3 level. Or in other words: all IP packets are forwarded. The "Allow_L3" rule set in the packet filter provides for that. By defining rule sets, which bar certain traffic and which are positioned in front of the "Allow_L3" rule set in the order of processing, exceptions from this treatment can be added. This treats the traffic like a "black list".

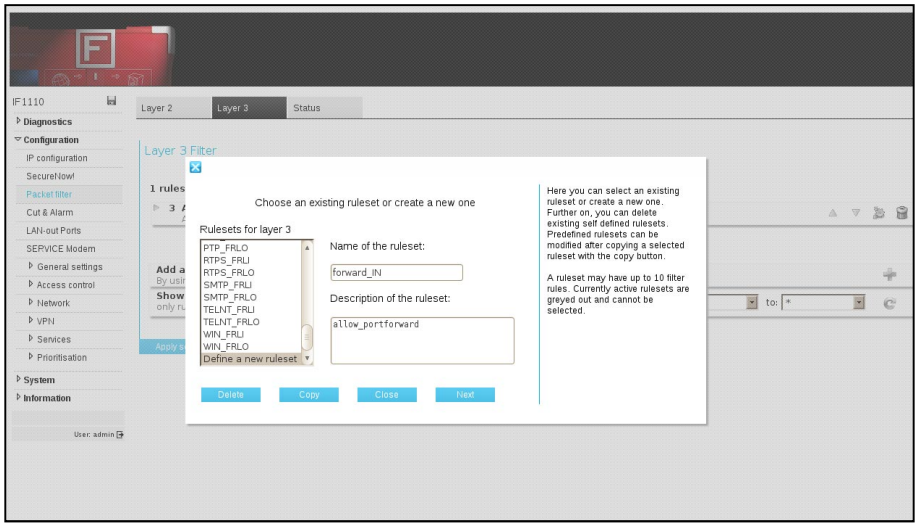
In the opposite case, traffic can be treated like with a white list, if the "Allow_L3" rule set is deleted. Rule sets which allow certain ("white") traffic must be added in this case. For this example, we will now explain how such a "white list" rule set is created.

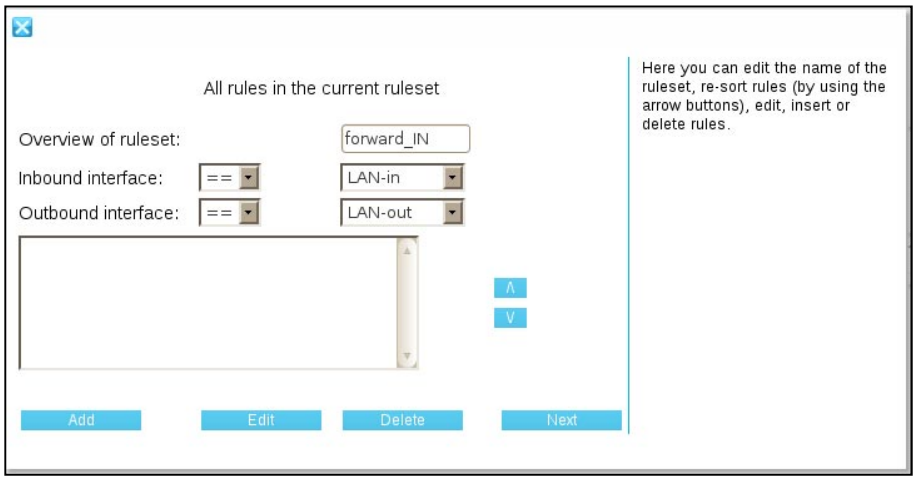
Note:

You'll find comprehensive information on how to control a packet filter in our "Packet filter" use case.

A new rule set must be defined by using the packet filter: it will allow the transmission of TCP packets to the host computer (192.168.253.162:9999 in this case).

First, you create a new rule set in the packet filter by using the Plus icon, and call it e.g. "forward_IN":

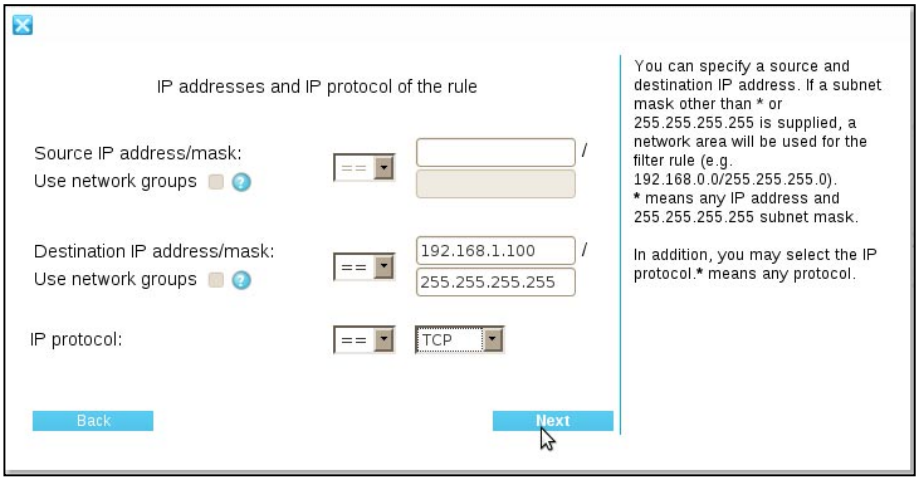




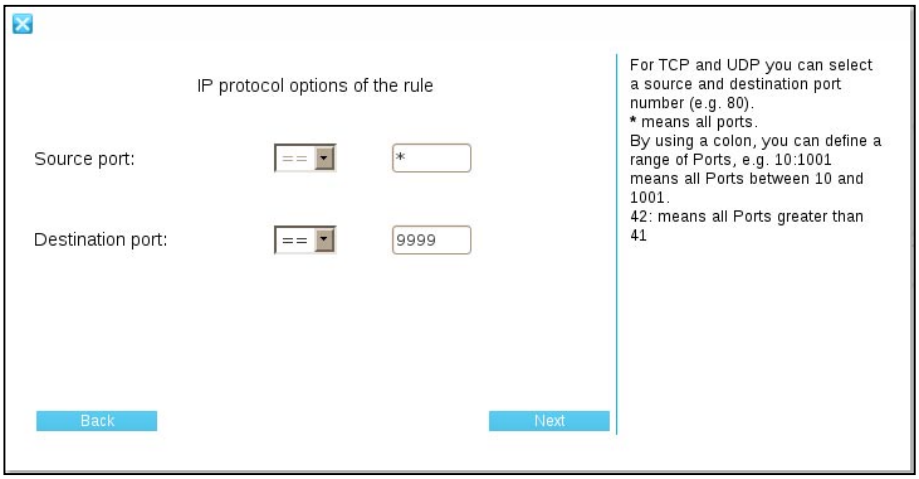
This rule set must verify the incoming packets (from LAN-in to LAN-out) of layer 3 (TCP/UDP packets) , which is why "LAN-in" is selected as the inbound interface and "LAN-out" as the outbound interface in the overview of rule sets.

By clicking on "Add", the process is continued with defining a rule for the rule set. This rule is to release the port not in general, but only for the corresponding computer, on which the TCP based service actually runs. The subnet mask 255.255.255.255 specified in the example means that only this single IP address is valid as a destination:

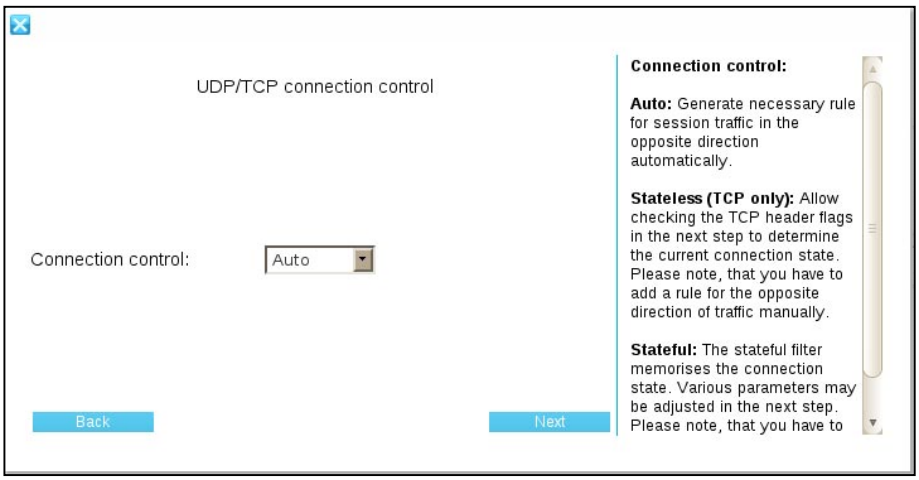
© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen


IP addresses and IP protocol of the rule
Source IP address/mask:
Use network groups
Destination IP address/mask:
Use network groups
192.168.1.100
255.255.255.255
IP protocol:
TCP
Back
Next
You can specify a source and destination IP address. If a subnet mask other than * or 255.255.255.255 is supplied, a network area will be used for the filter rule (e.g. 192.168.0.0/255.255.255.0).
* means any IP address and 255.255.255.255 subnet mask.
In addition, you may select the IP protocol.* means any protocol.

Apart from the destination IP address, the port must also be an exact match.

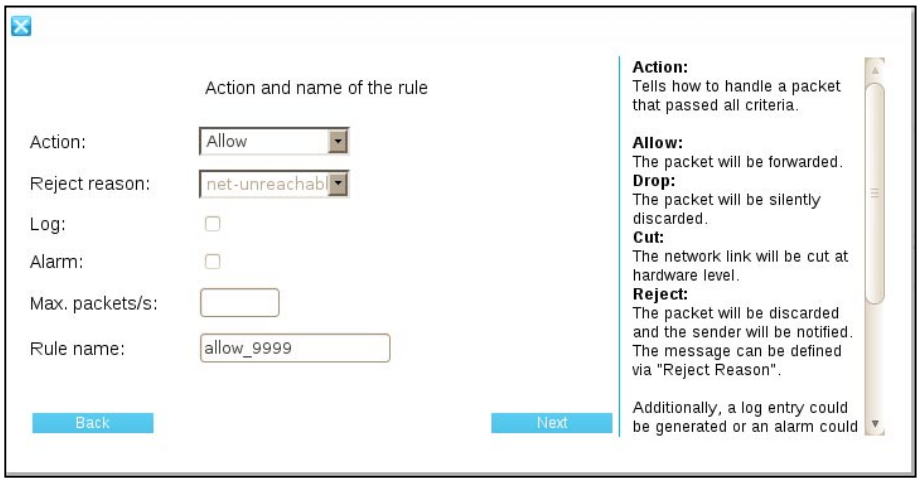

IP protocol options of the rule
Source port:
Destination port:
9999
Back
Next
For TCP and UDP you can select a source and destination port number (e.g. 80).
* means all ports.
By using a colon, you can define a range of Ports, e.g. 10:1001 means all Ports between 10 and 1001.
42: means all Ports greater than 41

"Auto" can be selected as a connection control method for rules concerning TCP connections. It saves you from creating a separate rule for the return direction of this connection.

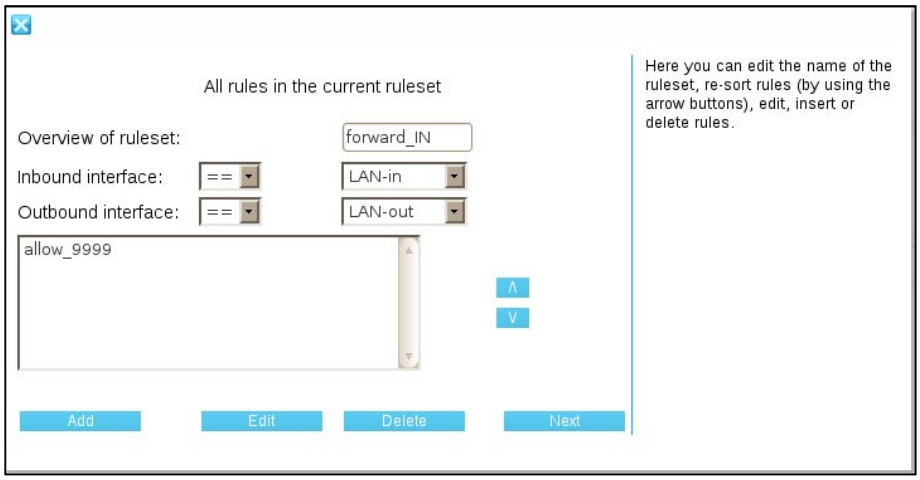

UDP/TCP connection control
Connection control:
Auto
Back
Next
Connection control:
Auto: Generate necessary rule for session traffic in the opposite direction automatically.
Stateless (TCP only): Allow checking the TCP header flags in the next step to determine the current connection state. Please note, that you have to add a rule for the opposite direction of traffic manually.
Stateful: The stateful filter memorises the connection state. Various parameters may be adjusted in the next step. Please note, that you have to

In the next step, we'll define what should happen with those packets which meet all of the criteria (i.e. with those packets directed to the 192.168.1.100:9999 address). The packets

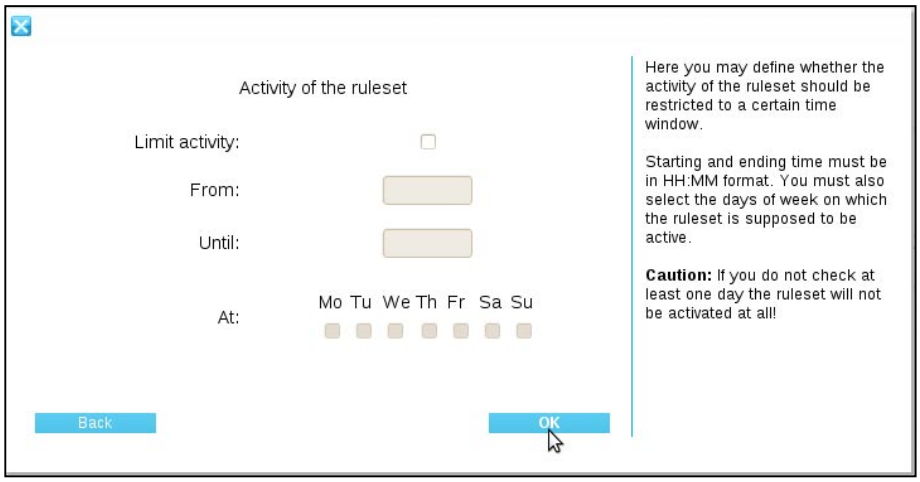
are allowed in this example. Additionally, the name of the rule is here defined (allow_9999):



The rule definition is now completed. An overview of this rule set is displayed next.



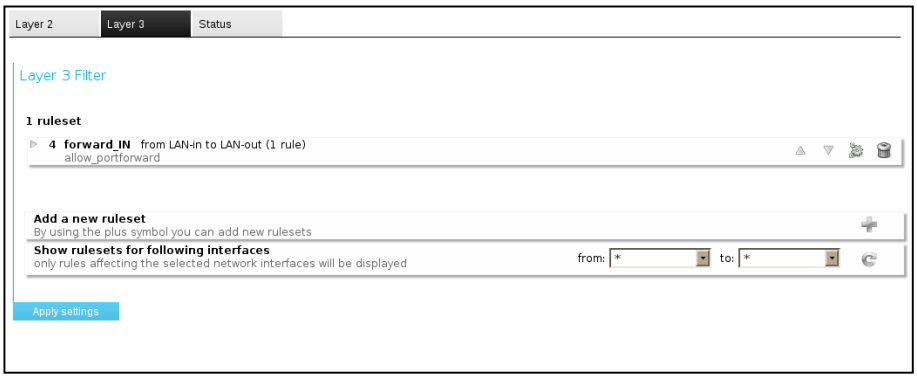
In the next step, the availability of the forwarding can be limited to a certain time window on certain days and the access to this service limited, as a result.


Activity of the ruleset
Limit activity:
From:
Until:
At:
Mo Tu We Th Fr Sa Su
Back
OK
Here you may define whether the activity of the ruleset should be restricted to a certain time window.
Starting and ending time must be in HH:MM format. You must also select the days of week on which the ruleset is supposed to be active.
Caution: If you do not check at least one day the ruleset will not be activated at all!

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

Finally, the rule set is enabled by clicking on "**OK**". As a result, the input window is closed, and the packet filter overview is displayed once more. If a "whitelist" behaviour is to be achieved, the "Allow_L3" rule set must still be deleted, so that only the new "forward_IN" entry is visible.

In the final step, all settings are saved including the changes by clicking on "**Apply Settings**".



11.5 VIRUS SCAN

GENERAL

Up to 50 directories shared via the network (the so-called shares or shared folders) can be addressed from a centralised computer by means of the firewall, in order to scan them for viruses with antivirus software.



Note:

Only files can be checked for viruses, but not the running processes and not the network traffic of the computer on which the shared folders are located!
Shared folders are only opened with read-only access permission. That means that although viruses can be diagnosed they can't be removed or healed!
Scanning via the network is slower than a local scan.

We assume for this use case, that the firewall runs in IP router mode, which means that it routes the traffic between two separate networks. The firewall is connected with the network 192.168.111.0/24 (includes computers with an 192.168.111.xxx IP address pattern) via LAN-in, and with the network 192.168.253.0/24 (includes computers with an 192.168.253.xxx IP address pattern) via the LAN-out interface. The network would be the same for both interfaces, if the Transbridge mode would be used. The firewall configuration and the virus scan are carried out by a computer called "Server", which is located in the 192.168.111.0/24 network.

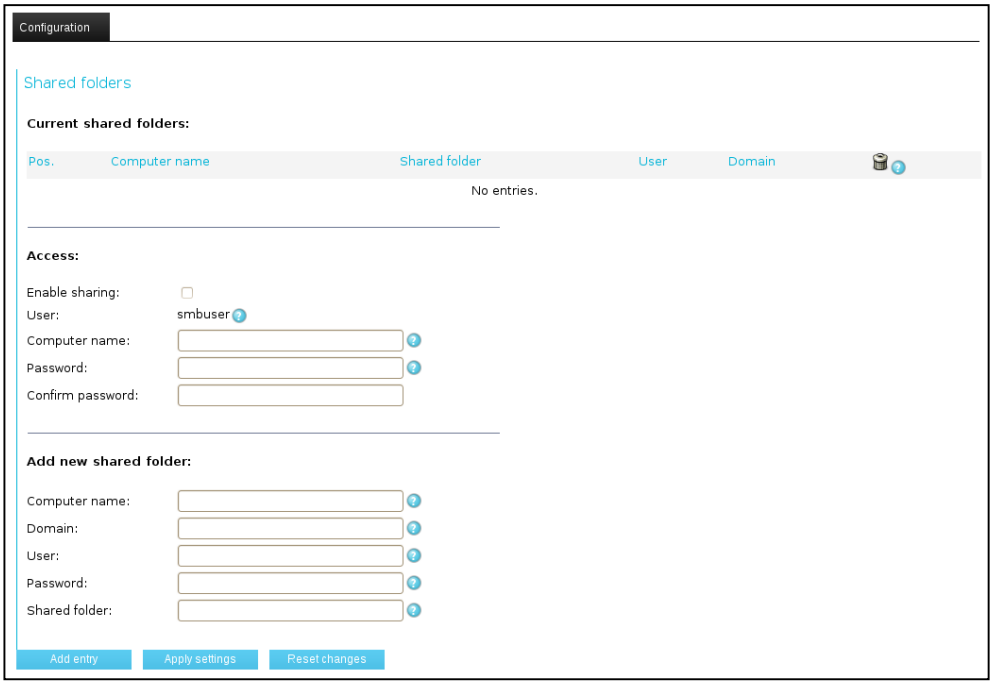


Note:

Computer names can only be resolved for computers in both directly connected networks.

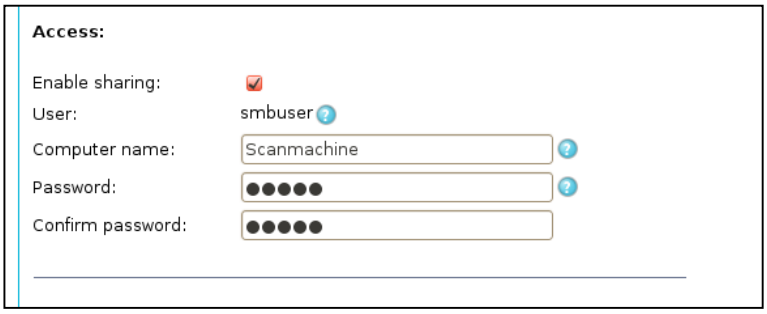
The list of shared folders and their access are set up in the "Firewall device/Services/Shared folders" menu. By default, this service is disabled.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen



SHARE ACCESS

The access is always made by the "smbuser" user, and is only permitted for the computer whose name is entered (or its IP address, alternatively). The password can freely be defined and is not based on the existing NT users. All changes are saved by clicking on "Apply Settings".

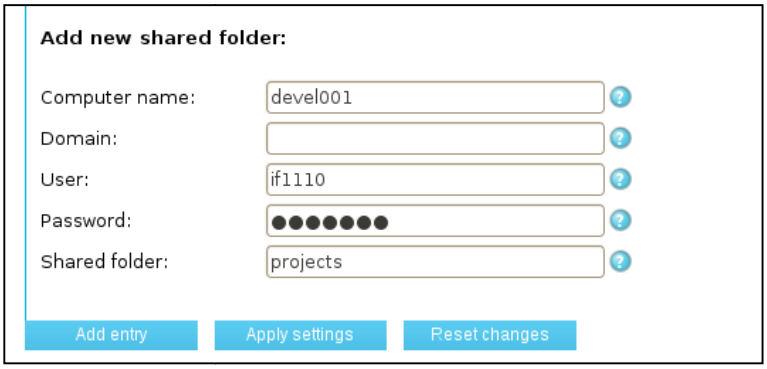


Note:

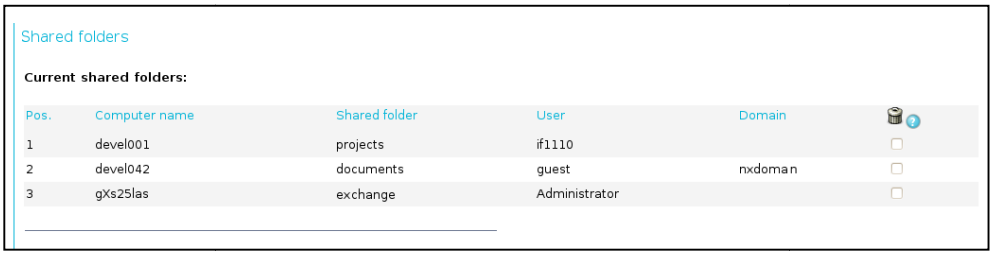
This service can entirely be disabled! Access is in fact only possible if "Enable sharing" is activated. Access is always of read-only type only, i.e. there are no write permissions for the shared folders!

ADDING SHARED FOLDERS

If you wish to add a new shared folder, the folder name, user name and password for this/these shared folder(s) must be known, as they have been defined on the local computer (user name and password of the user's Windows login). The computer name can alternatively be an IP address. Specifying the domain is recommended, but is not necessarily required under certain circumstances.



By clicking on "Add Entry", the entry is added to the list, which then looks, for instance, as shown below:



Note:

Passwords should only be disclosed to the administrator!
The user with whose account the shared folder is configured must have write permission for the shared folder, in order to allow the virus scanner programme to make any changes! That means, if for instance "Administrator"" is used as shared folder user, the "Administrator" user on the computer with the shared folder must have write access for this/these shared folder(s).
If defining a shared folder fails (is only attempted if the service is enabled), an error message is sent, but the definition is saved (for the event that the computer e.g. was temporarily shut down). Simply disable, and then immediately enable the service, if you'd like to access this share later (once the computer is restarted).
If the "No such share" error occurs for a certain share, try entering the entire name again but with all small letters, since some Windows versions have an issue with capital letters.

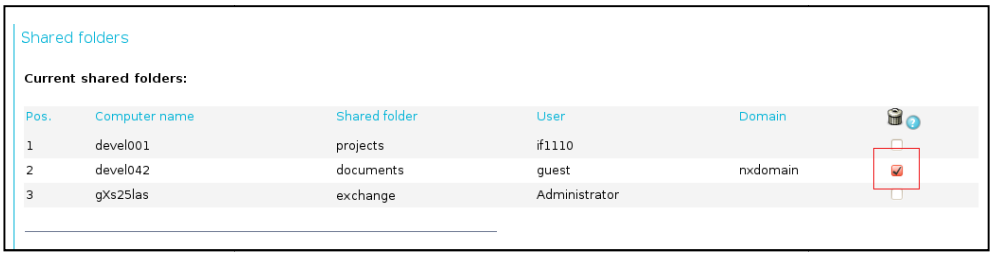
© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

DELETING SHARED FOLDERS

Simply tick the box to the right of the corresponding entry (underneath the trash can icon) and then push "Apply settings", if you'd like to delete a shared folder.

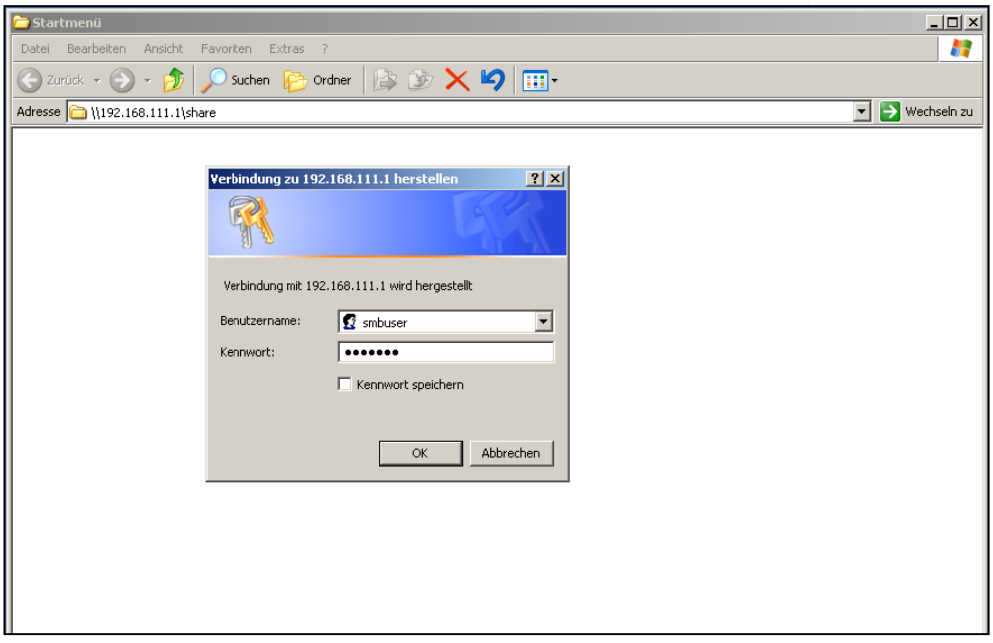
Note:

If more than one entry is to be deleted, the share service should be disabled first (untick the "Enable sharing" option and then push "Apply settings"), and only be enabled after the changes have been made, since updating the list could take a very long time with the service enabled!

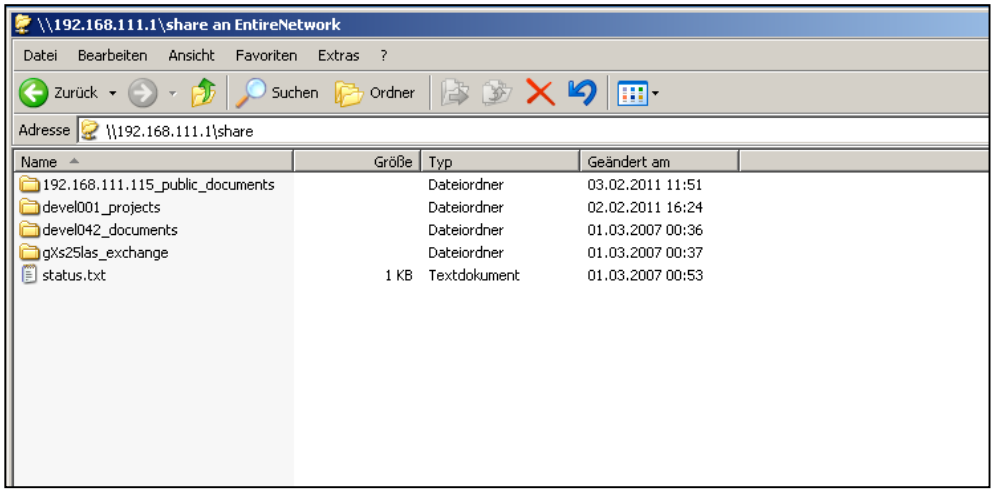


ACCESS VIA WINDOWS EXPLORER

Open Windows Explorer and activate the "share" network directory of the firewall. Here, the actual IP address of the firewall must directly be used (you can e.g. read it from the display). In our use case, the firewall has the IP address 192.168.111.1 at the LAN-in interface. This means that you have to specify "\\192.168.111.1\share" in the address bar of the Windows Explorer. During authentication, the user is always called "smbuser" and the password corresponds with the one defined for share access.



If the user authentication was successful, a list with the shared folders and additionally a "status.txt" file appears. This file includes an error message, if not all shared folders were successfully addressed (e.g. because of the wrong password).

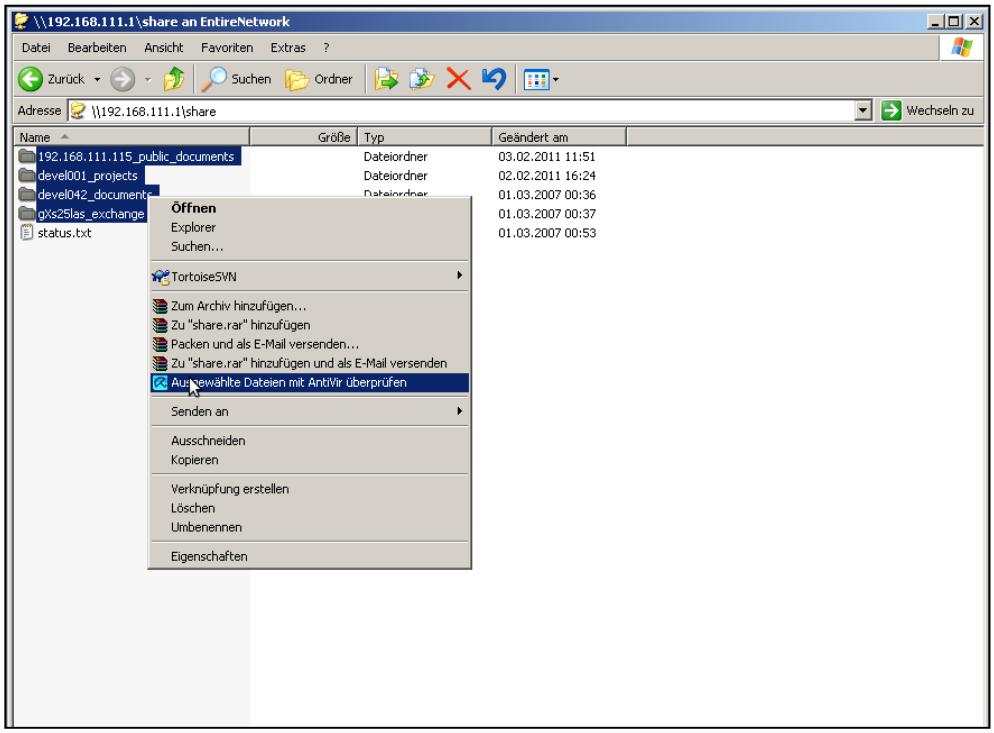

\\192.168.111.1\share an EntireNetwork
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Ordner
Adresse \\192.168.111.1\share
Name Größe Typ Geändert am
192.168.111.115_public_documents Dateiordner 03.02.2011 11:51
devel001_projects Dateiordner 02.02.2011 16:24
devel042_documents Dateiordner 01.03.2007 00:36
gXs25las_exchange Dateiordner 01.03.2007 00:37
status.txt 1 KB Textdokument 01.03.2007 00:53

Note:

Authentication under Windows can sometimes fail accompanied with the error message "Share not found" despite having correctly entered the share name. Should this happen, please proceed according to the instructions given in the "Network drive mapping" section, and address the share as a network drive.
The "status.txt" file must be opened with WordPad, because it is not correctly represented in the editor.

VIRUS SCAN VIA WINDOWS EXPLORER

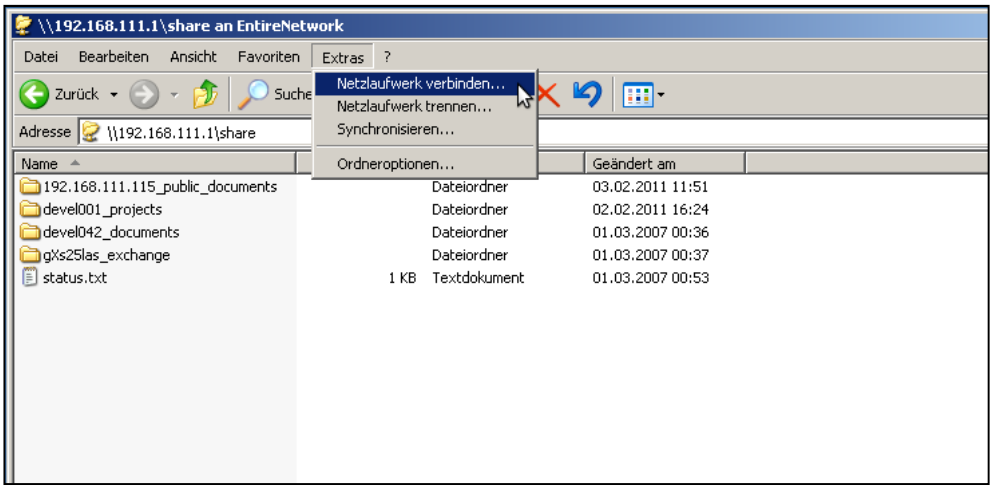
If the antivirus software has created an entry in the Explorer, first select all shares (CTRL-A), and then right-click on the corresponding menu entry.



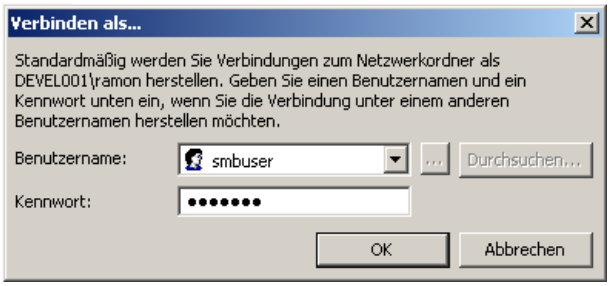
© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

NETWORK DRIVE MAPPING

Should the antivirus software not allow the direct use of network folders as a scan target, then you can turn such a network folder into a local drive by using "Tools / Map network drive"




Netzlaufwerk verbinden
Windows ermöglicht Ihnen, die Verbindung mit einem freigegebenen Netzwerkordner herzustellen. Durch Zuweisen eines Laufwerkbuchstabens an die Verbindung können Sie über "Arbeitsplatz" auf den Ordner zugreifen.
Bestimmen Sie den Laufwerkbuchstaben für die Verbindung und den Ordner, mit dem die Verbindung hergestellt werden soll:
Laufwerk: Y:
Ordner: \\192.168.111.1\share
Durchsuchen...
Beispiel: \\Server\Freigabe
Verbindung bei Anmeldung wiederherstellen
Verbindung unter anderem Benutzernamen herstellen
Onlinespeicherplatz anfordern oder mit einem Netzwerkserver verbinden
< Zurück
Fertig stellen
Abbrechen


Verbinden als...
Standardmäßig werden Sie Verbindungen zum Netzwerkordner als DEVEL001\ramon herstellen. Geben Sie einen Benutzernamen und ein Kennwort unten ein, wenn Sie die Verbindung unter einem anderen Benutzernamen herstellen möchten.
Benutzername: smbuser
Durchsuchen...
Kennwort: •••••••
OK
Abbrechen

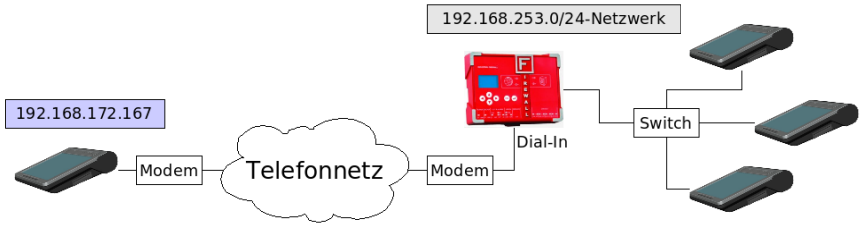
Note:

The user must be set to "smbuser" and the corresponding password must be set as well by using the "Connect with different user name" option.
If a virus scan is to be used after login, the "Reconnect on logon" option must be set.

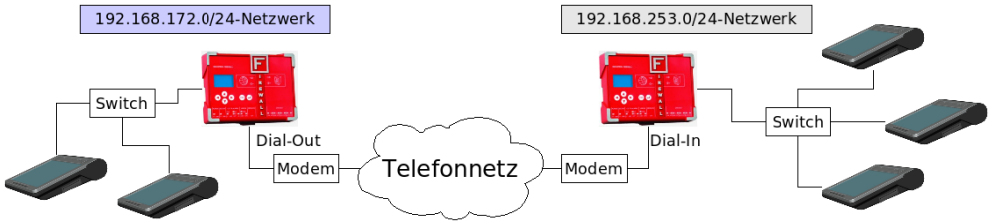
11.6 SERVICE

GENERAL

Dialling in or out (Dial-In/Out) via the firewall SERVICE port can be done by using a modem. If SERVICE is configured as Dial-In, an external device can dial in into the LAN-in or LAN-out network of the firewall. Only a single LAN (e.g. 192.168.253.0/24) exists in Transbridge mode.



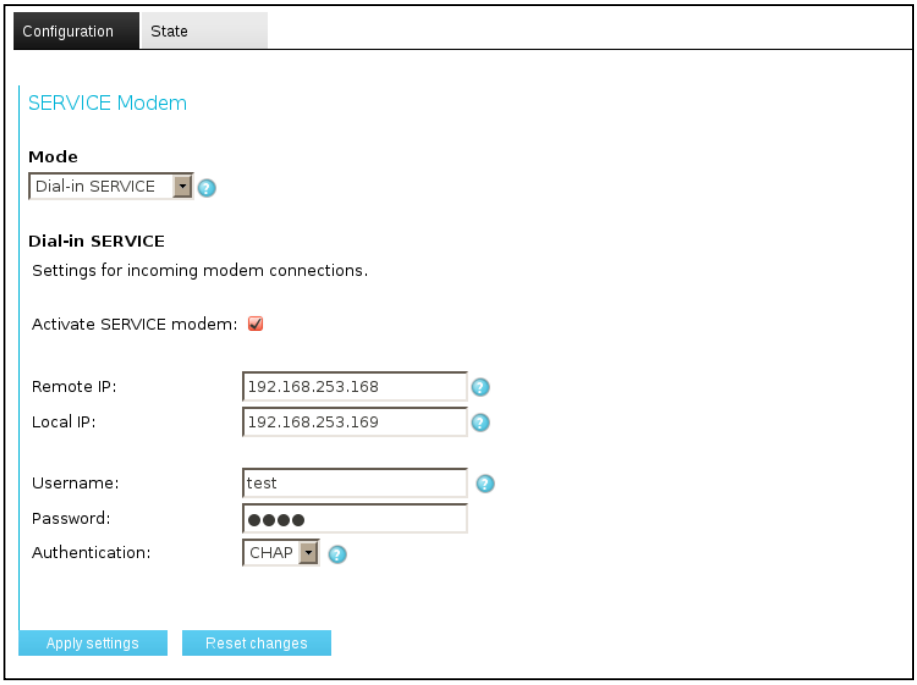
If SERVICE is configured as Dial-Out (and if the remote device, e.g. a firewall is in Dial-In mode), then the Dial-Out firewall acts as the router for connecting with the network of the remote device (e.g. of a Dial-In firewall).



SERVICE CONFIGURATION AS DIAL-IN

"Dial-In SERVICE" is selected as the mode in the "General Settings/Interfaces/SERVICE" menu. The "Remote IP" is assigned to the remote device once the connection is established, whereas the "Local IP" represents the IP address of the local remote transmission endpoint (PPP endpoint). Furthermore, the user name and password, with which the dial-in device has to be authenticated, must be specified.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

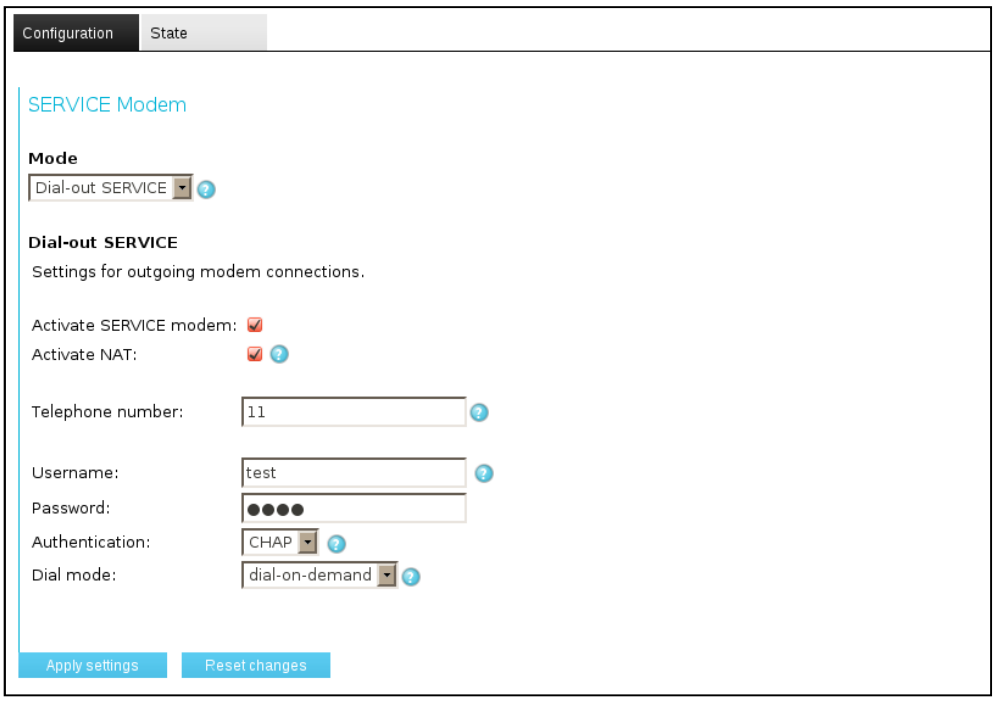


Note:

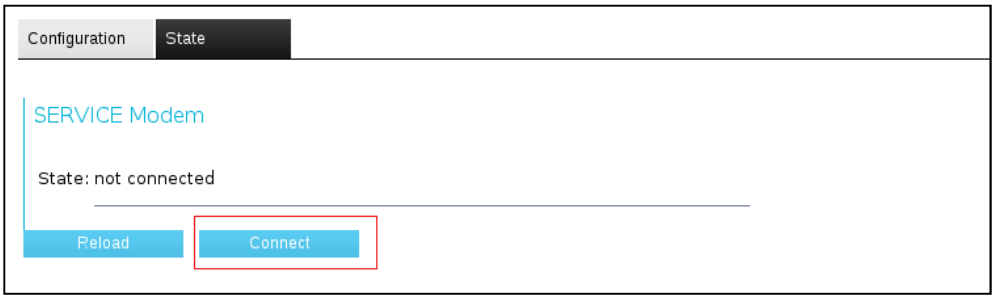
The "Remote IP" and the "Local IP" must both originate from either the LAN-in or LAN-out network. That means the device which dials in is connected with one of both networks (except in Transbridge mode, where there is only a single network, that is e.g. 192.168.253.0/24).

SERVICE CONFIGURATION AS DIAL-OUT

In this case, the mode is set to "Dial-Out SERVICE", and the phone number of the remote device is specified (an internal telephone system was used in this example, in which the modem of the Dial-Out firewall had extension number 11). User name and password must match the data specified in the Dial-In configuration. If "dial-on-demand" is used, the connection is established as soon as the firewall can no longer forward a data packet because the route is missing. The remote transmission connection then also acts as the default gateway.



In the "manual" dialling mode, the connection can manually be established or terminated in the "Diagnostics/SERVICE" menu item.



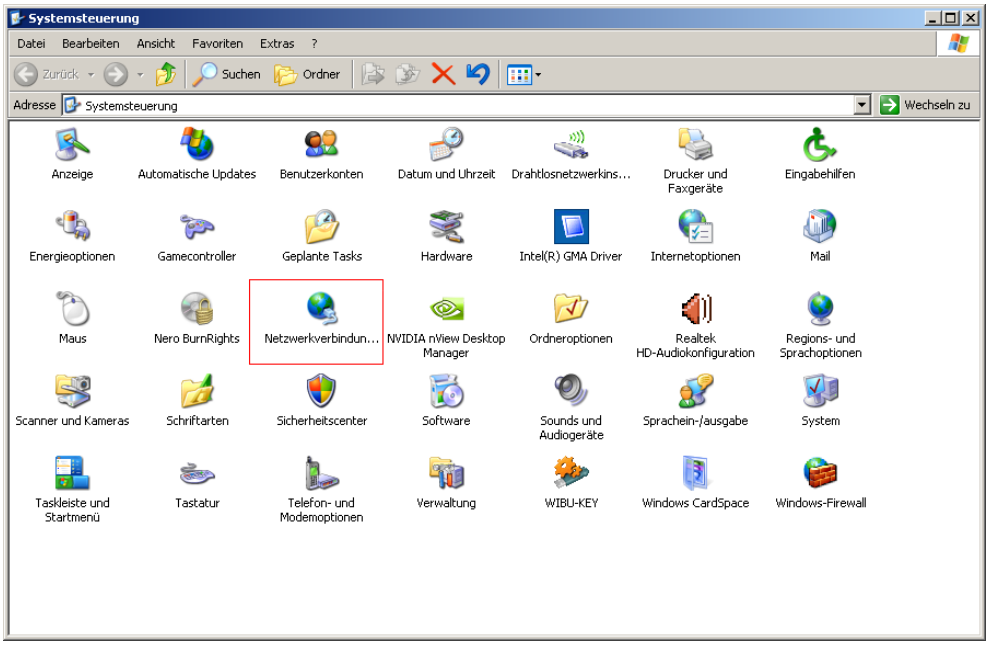
Note:

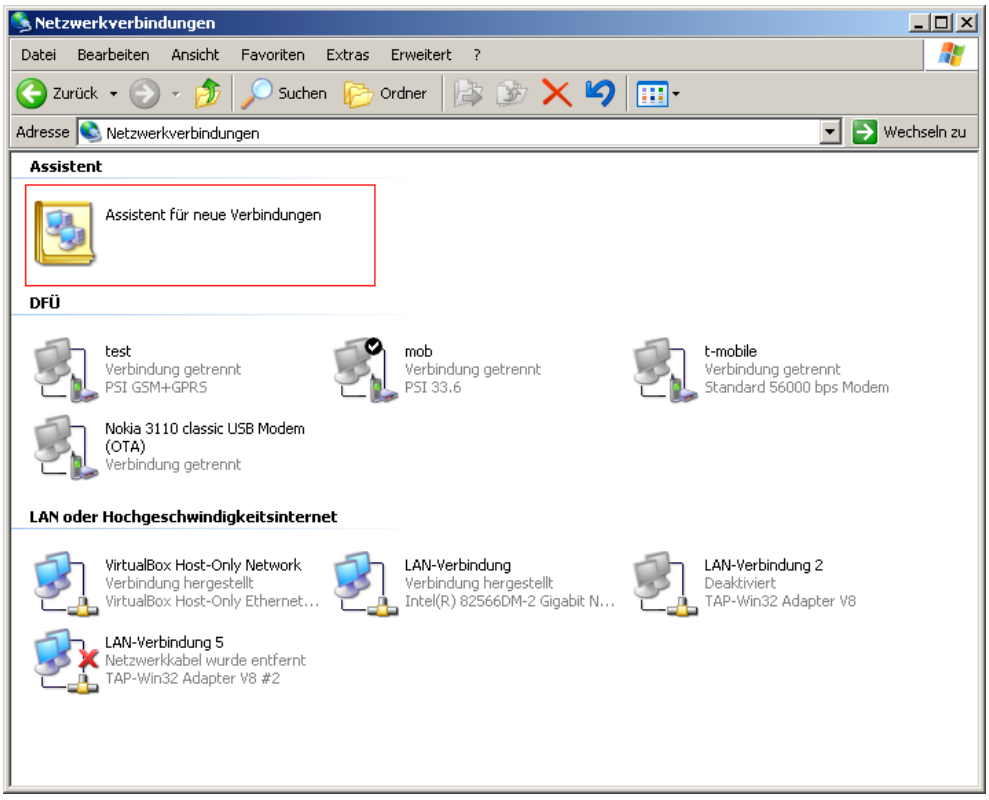
The "Remote IP" assigned by the remote device must never be located in any of both networks (LAN-in as well as LAN-out, or LAN only in Transbridge mode), since otherwise the routing via the remote transmission connection cannot work.

PC CONFIGURATION AS DIAL-OUT

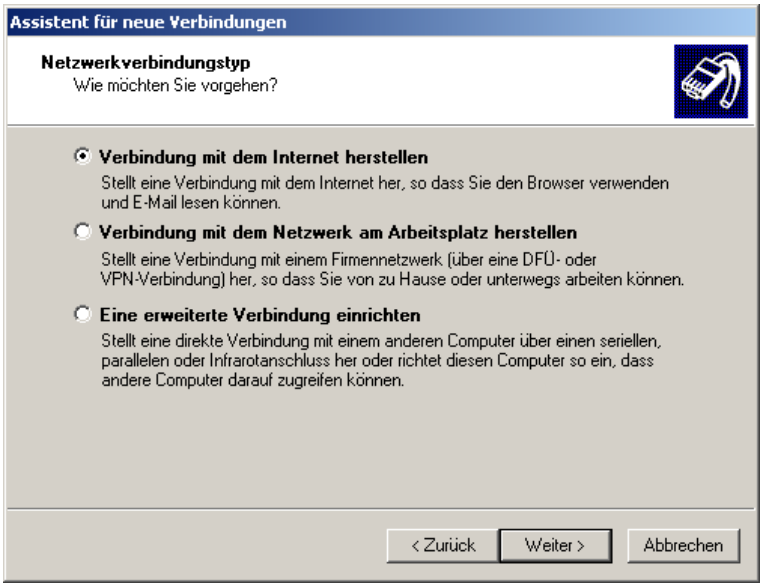
If you, for instance, want to dial in with a standard laptop and with an integrated modem, you'll have to define a connection for remote transmission in the "Control panel" menu, "Network connections" menu item, by using the "New connection" wizard.

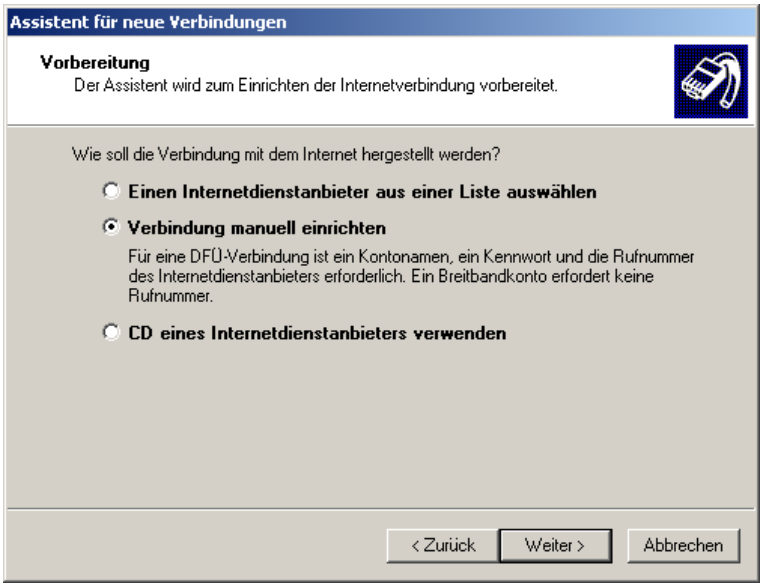
© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

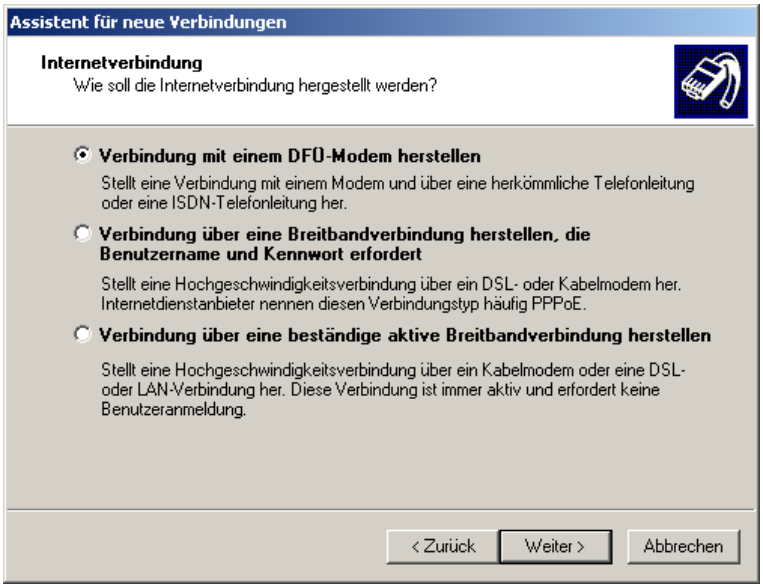




In the wizard, you'll have to set up an Internet connection via modem access. Any name can be chosen for the name of the connection. User name and password must match the data specified in the Dial-In configuration of the firewall.


Assistent für neue Verbindungen
Netzwerkverbindungstyp
Wie möchten Sie vorgehen?
Verbindung mit dem Internet herstellen
Stellt eine Verbindung mit dem Internet her, so dass Sie den Browser verwenden und E-Mail lesen können.
Verbindung mit dem Netzwerk am Arbeitsplatz herstellen
Stellt eine Verbindung mit einem Firmennetzwerk (über eine DFÜ- oder VPN-Verbindung) her, so dass Sie von zu Hause oder unterwegs arbeiten können.
Eine erweiterte Verbindung einrichten
Stellt eine direkte Verbindung mit einem anderen Computer über einen seriellen, parallelen oder Infrarotanschluss her oder richtet diesen Computer so ein, dass andere Computer darauf zugreifen können.
< Zurück
Weiter >
Abbrechen


Assistent für neue Verbindungen
Vorbereitung
Der Assistent wird zum Einrichten der Internetverbindung vorbereitet.
Wie soll die Verbindung mit dem Internet hergestellt werden?
Einen Internetdienstanbieter aus einer Liste auswählen
Verbindung manuell einrichten
Für eine DFÜ-Verbindung ist ein Kontonamen, ein Kennwort und die Rufnummer des Internetdienstanbieters erforderlich. Ein Breitbandkonto erfordert keine Rufnummer.
CD eines Internetdienstanbieters verwenden
< Zurück
Weiter >
Abbrechen


Assistent für neue Verbindungen
Internetverbindung
Wie soll die Internetverbindung hergestellt werden?
Verbindung mit einem DFÜ-Modem herstellen
Stellt eine Verbindung mit einem Modem und über eine herkömmliche Telefonleitung oder eine ISDN-Telefonleitung her.
Verbindung über eine Breitbandverbindung herstellen, die Benutzername und Kennwort erfordert
Stellt eine Hochgeschwindigkeitsverbindung über ein DSL- oder Kabelmodem her. Internetdienstanbieter nennen diesen Verbindungstyp häufig PPPoE.
Verbindung über eine beständige aktive Breitbandverbindung herstellen
Stellt eine Hochgeschwindigkeitsverbindung über ein Kabelmodem oder eine DSL- oder LAN-Verbindung her. Diese Verbindung ist immer aktiv und erfordert keine Benutzeranmeldung.
< Zurück
Weiter >
Abbrechen

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen



Note:

Should the computer be integrated in a LAN or WLAN, the IP address of the remote transmission PPP interface must never be located in any of the previously configured networks, since otherwise the routing does not work correctly (you can recognise it by the fact that the remote network cannot be reached although the connection for remote transmission has been established without errors). The network in question is then either temporarily to be disabled, or the routing table to be adapted.
If error 680 ("No dial tone") occurs, the "Wait for dial tone" modem option in the control panel must be disabled.

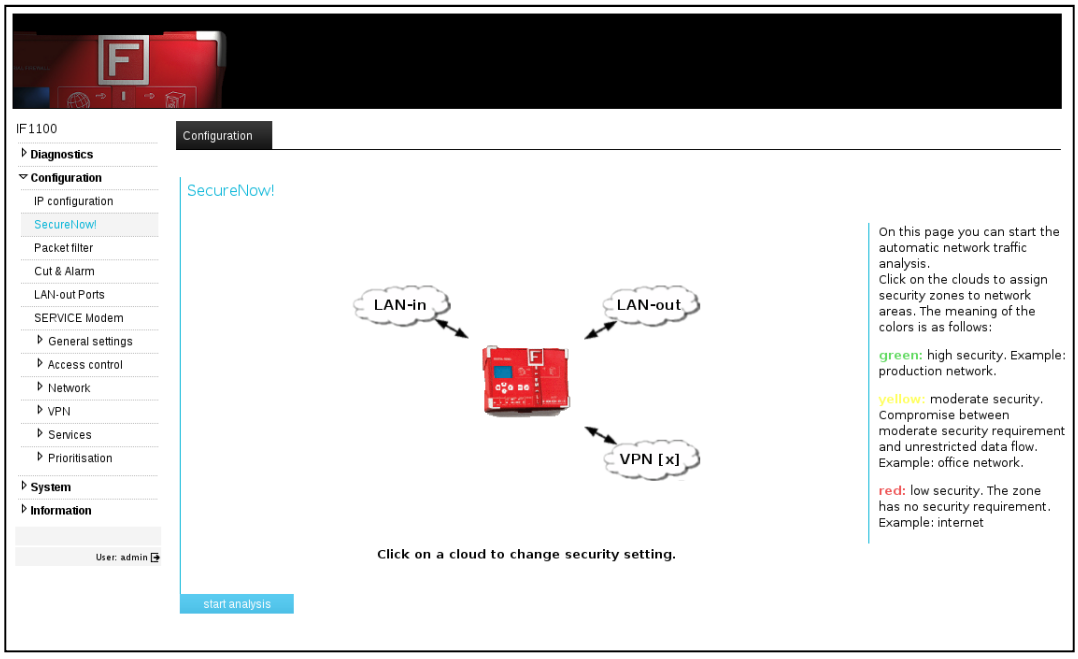
11.7 SECURENOW!

GENERAL

SecureNow! enables everybody to achieve a maximum level of security for local networks with very little interaction. SecureNow! analyses the network traffic, which goes through the Industrial Firewall, and generates tailored filter rules for ebtables (in Transbridge mode) or iptables (in IP router or IP router extended mode) based on this information.

START PAGE

At the start, the user defines for all active interfaces of the IF1xxx device, which security requirements should apply. Here you can chose from three different levels: High, moderate, and low. SecureNow! creates particularly strict rules for the zones with "high" security level. Rules are less strict with the "moderate" level, in order to accommodate for requirements like they usually occur in, let's say, office networks. The "low" security level should be selected for the uplink, e.g. for the interface with the Internet. On the one hand, the rules for this zone are strict when it comes to the traffic originating from this zone. But on the other hand, the traffic originating from a zone with a higher security level and directed to a zone with lower security level, is always permitted if in doubt - i.e. this always applies to the lowest level.
Network traffic, which has been recognised as security critical items, is treated as an exception. SecureNow! has an integrated database, in which frequently used protocols are evaluated with respect to their security.

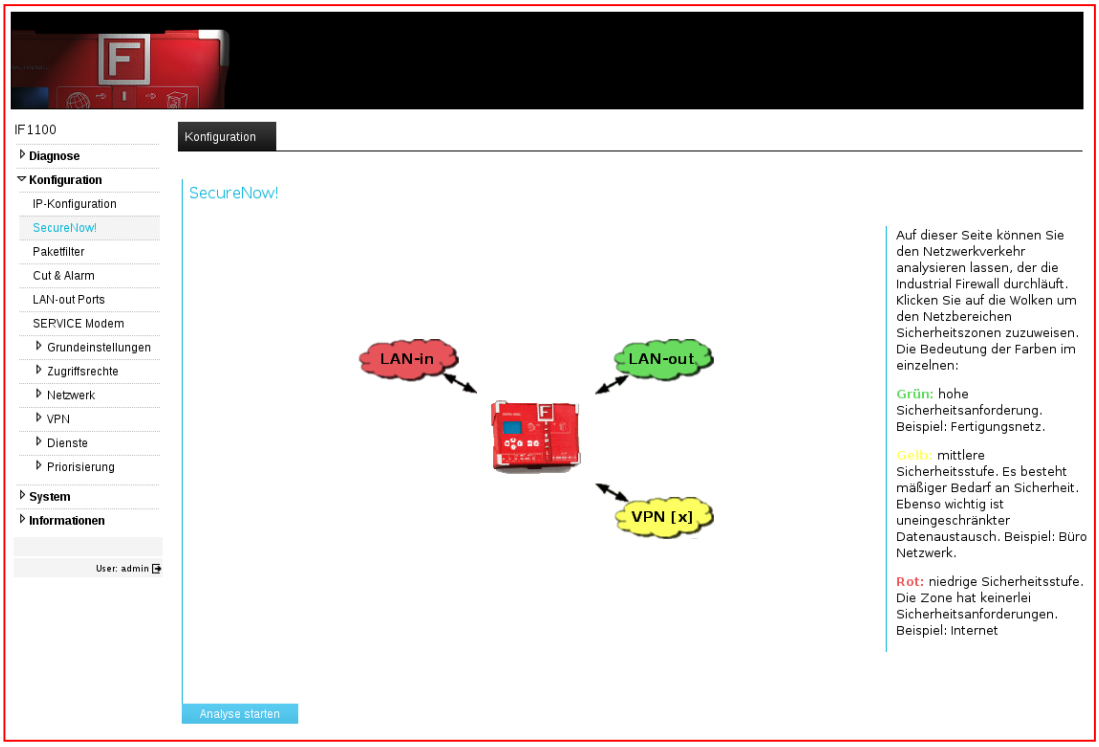


The user can switch from one security level to another by clicking on one of the clouds with the mouse. On the right-hand side, you'll find notes which explain the significance of these zones by using examples.

Note:

If two networks are highlighted by using the same colour (e.g. yellow), rules for the traffic between these zones will allow all packets.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen



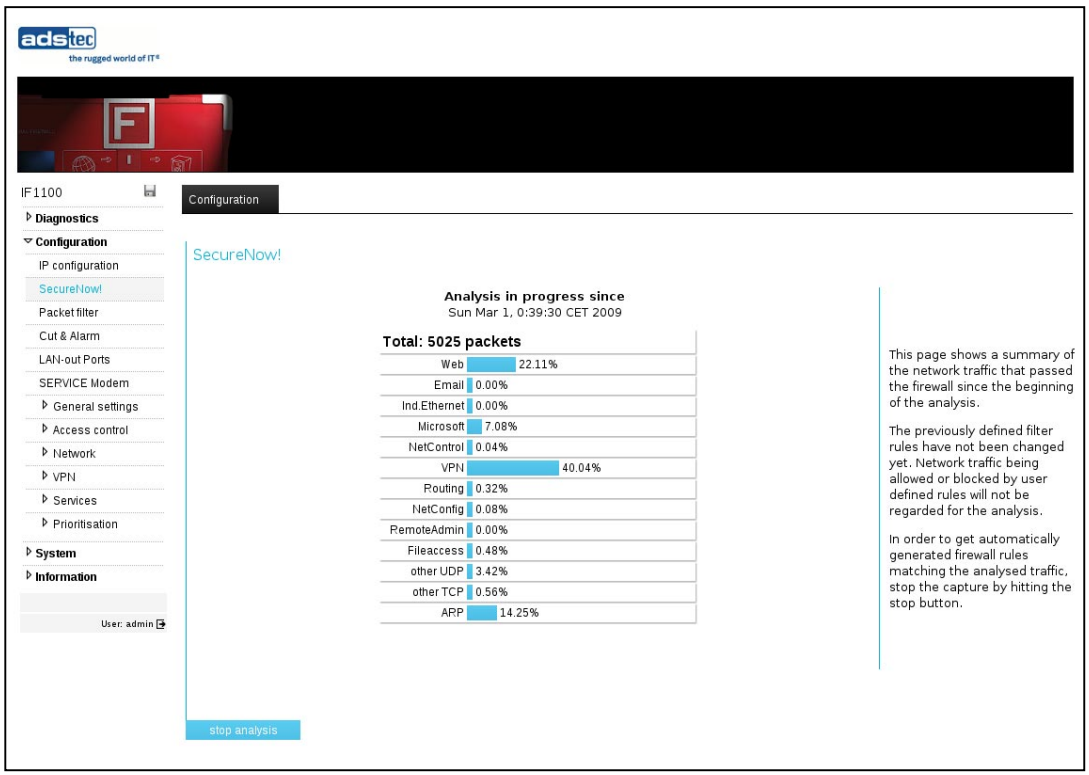
Once the security zones are configured, the user starts the analysis phase by clicking on "**Start analysis**". Network traffic will not be affected by SecureNow! during this phase. The protocol information of data packets is saved in a structured approach and in an efficient way by SecureNow!.

TRAFFIC STATISTICS

During this period, the user can see a traffic statistics window, which shows at a glance which network traffic classes have which share in the overall data traffic.

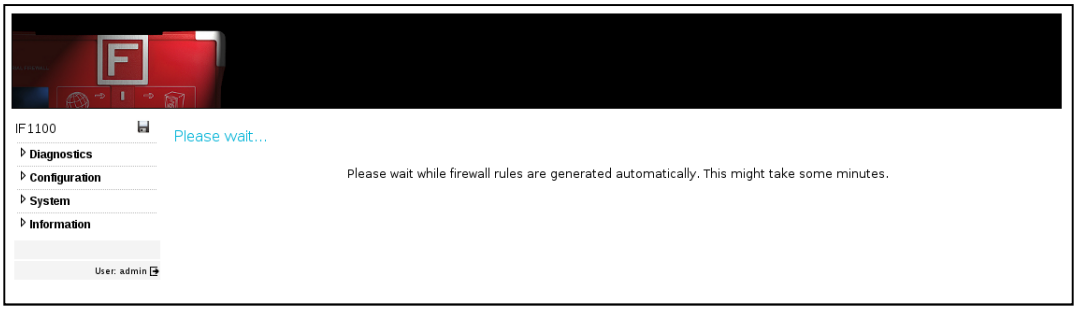
Note:

The percentages shown in the traffic statistics window may differ from the data shown in the result overview (see further below), if filter rules have previously been enabled. The traffic statistics window shows all packets which pass through the firewall, whereas SecureNow! only displays the packets which have not been covered by any of the previously defined rules.



The user can finish the recording phase at any point in time. After that, the recorded network traffic is analysed and filter rules are generated.

Any time period can be chosen for the duration for the recording phase. It should, however, be chosen in such a way that a representative proportion of traffic can be analysed. Selecting a duration of 24 hours usually is reasonable, unless the network traffic differs a lot from day to day.

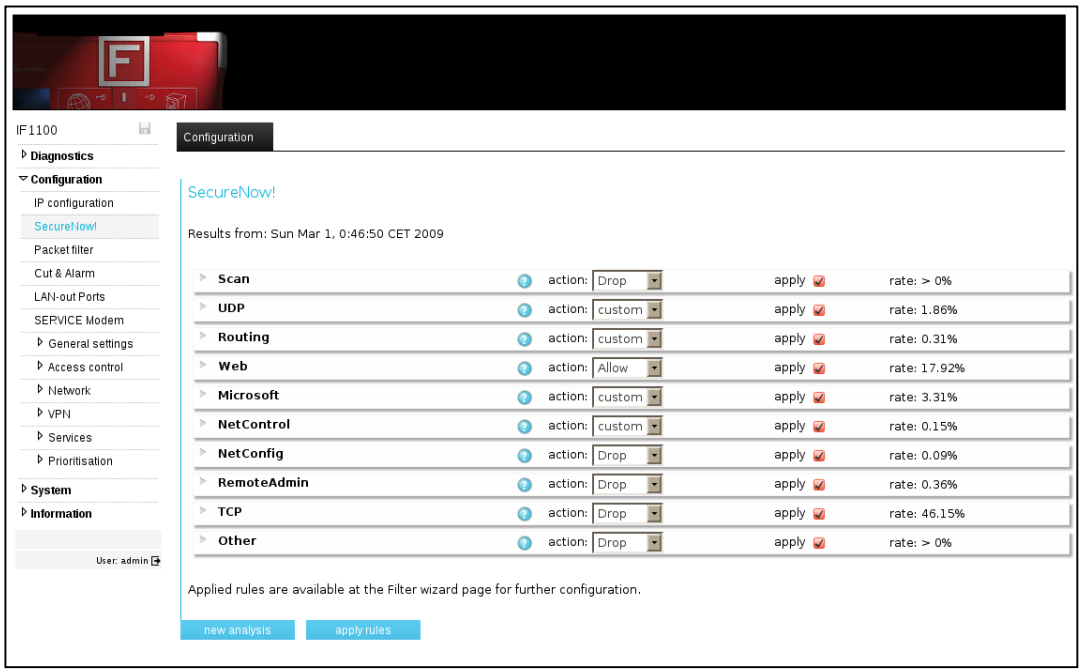


After clicking on "**Stop analysis**", filter rules are automatically created. Creating the rules can take up to several minutes, depending on the recording time and on the number and variance of the monitored data packets.

These rules are subsequently presented on an overview page, where the user has the opportunity of partially modifying or saving some individual rules.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

RESULT PAGE



The rules are divided into several classes, which have already been used in the traffic statistics page shown before. If you click on one of the classes, the rules included in this class are displayed in the detailed view.

There is one special class: „**Scan**". Rules are listed here, which are destined to completely bar certain network subscribers purely because of the IP address used. The basis for this action is a detected port scan of this subscriber. Since ports scans are frequently used for detecting weaknesses of individual computers, it must be assumed that this type of subscriber poses a security threat. IP packets coming from this source are therefore completely discarded.

Note:

Some applications, such as Bittorrent, establish a large number of connections with different subscribers. The same applies to some servers, which provide a large number of services. This behaviour cannot be distinguished from a port scan by using SecureNow!. Should this be the case and this traffic be desired, the scan rule should simply be set to "Allow".

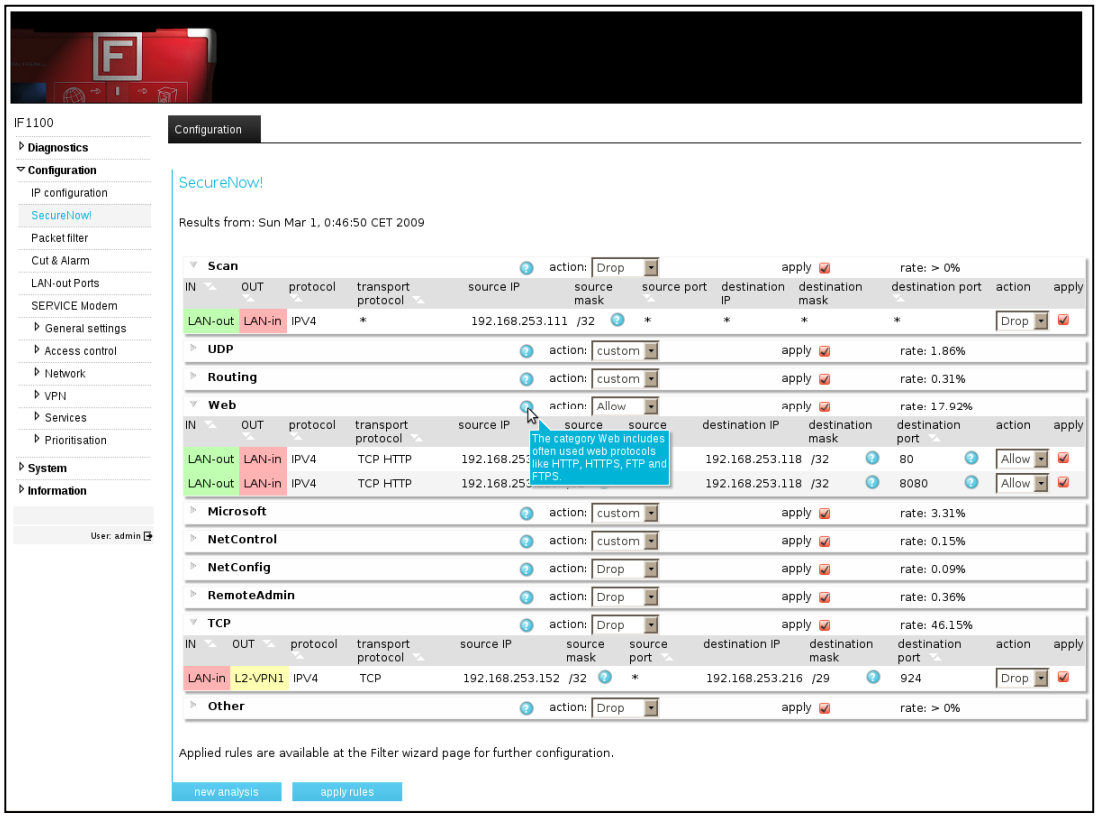
By using the class control bar, all included rules can be selected ("apply") or unselected. Additionally it is possible to modify the action for all included rules at once. "Allow" means that all affected packets may pass through the firewall. All packets are discarded with "Drop". "Custom" means that the rules within this class use different (customised) actions.

Note:

If the action is modified, you'll have to consider that other rules could probably still allow or bar a portion of the packets affected by this modification afterwards. It could, for example, happen that one rule checks a certain protocol first for an individual IP address and then another rule with the same protocol defines an action for an IP address range, which includes the IP address from the first rule. This would mean the first rule is a special case of the second rule. If this is the case, then both rules have the same previously defined action.

For the user, this means in detail: If a previously defined action is modified, all special cases further up in the order might have to be considered as well, and the associated actions might also have to be changed, if required.

The order, in which these rules are executed, corresponds with the order on the result page at the start, i.e. the more specific rules are placed further up in the list, and are always checked before the more general rules.

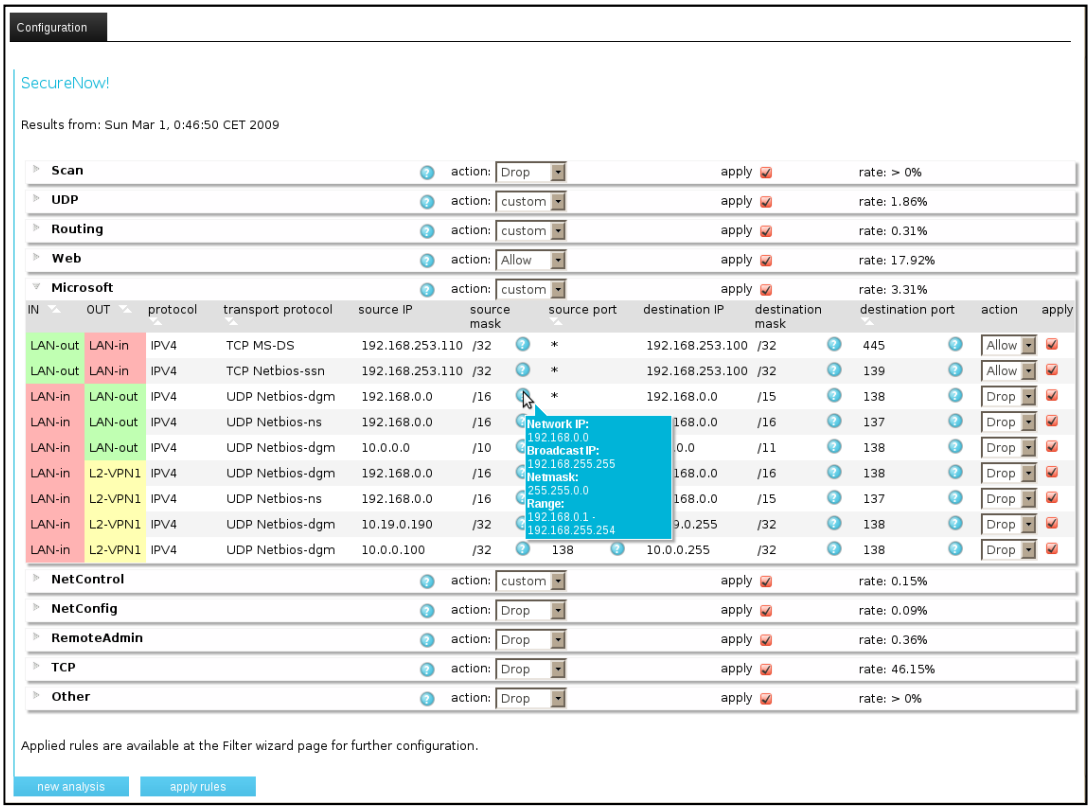


In the detailed view of rules it is always possible to sort the entries in lexicographical order by using different properties. In this case, the column header is an icon with two small white arrows. The rules of this class can be sorted in ascending or descending order, depending on the selected property, by clicking on the icon.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

SIGNIFICANCE OF COLUMNS IN THE DETAILED VIEW

In: This rule only applies to packets arriving on this port.
Out: This rule only applies to packets leaving this interface of the firewall.
protocol: In Transbridge mode, the layer 3 protocol, i.e. the ethertype priority of the rule is displayed here. The layer 4 protocol is displayed here with the regular or extended IP router mode.
transport protocol: (Is only shown in Transbridge mode). Here, you'll find the layer 4 protocol (e.g. UDP or TCP), if available.
source IP / source mask: This rule only applies to packets, which originate from an IP address of the network range, which is defined by the IP address and mask specified here. The user can obtain a more detailed explanation of this range by using the Help icon next to the net mask.
destination IP / destination mask: This rule only applies to packets, which are sent to an IP address of the network range, which is defined by the IP address and mask specified here.
source / destination port: In the event that TCP or UDP packets are used, the port number is specified in this place. Sometimes, the "*" symbol is used here, which represents all possible port numbers.
action: The destination address of the rule is defined here, i.e. it defines what should happen with the packets characterised by the previously specified criteria. You can chose between "Allow" and "Drop". Allow means that the packets are allowed to pass the firewall. Drop means that these packets are discarded.
apply: Individual rules can be selected for use by checking this checkbox individually. This requires that "apply rules" is finally pushed to confirm the changes. Affected rules are no longer displayed on this page afterwards. But they'll be still available for detailed configuration on the "Packet filter" page.


Configuration
SecureNow!
Results from: Sun Mar 1, 0:46:50 CET 2009
Scan action: Drop apply rate: > 0%
UDP action: custom apply rate: 1.86%
Routing action: custom apply rate: 0.31%
Web action: Allow apply rate: 17.92%
Microsoft action: custom apply rate: 3.31%
IN OUT protocol transport protocol source IP source mask source port destination IP destination mask destination port action apply
LAN-out LAN-in IPV4 TCP MS-DS 192.168.253.110 /32 * 192.168.253.100 /32 445 Allow
LAN-out LAN-in IPV4 TCP Netbios-ssn 192.168.253.110 /32 * 192.168.253.100 /32 139 Allow
LAN-in LAN-out IPV4 UDP Netbios-dgm 192.168.0.0 /16 * 192.168.0.0 /15 138 Drop
LAN-in LAN-out IPV4 UDP Netbios-ns 192.168.0.0 /16 168.0.0 /16 137 Drop
LAN-in LAN-out IPV4 UDP Netbios-dgm 10.0.0.0 /10 0.0 /11 138 Drop
LAN-in L2-VPN1 IPV4 UDP Netbios-dgm 192.168.0.0 /16 168.0.0 /16 138 Drop
LAN-in L2-VPN1 IPV4 UDP Netbios-ns 192.168.0.0 /16 168.0.0 /15 137 Drop
LAN-in L2-VPN1 IPV4 UDP Netbios-dgm 10.19.0.190 /32 9.0.255 /32 138 Drop
LAN-in L2-VPN1 IPV4 UDP Netbios-dgm 10.0.0.100 /32 138 10.0.0.255 /32 138 Drop
Network IP: 192.168.0.0
Broadcast IP: 192.168.255.255
Netmask: 255.255.0.0
Range: 192.168.0.1 - 192.168.255.254
NetControl action: custom apply rate: 0.15%
NetConfig action: Drop apply rate: 0.09%
RemoteAdmin action: Drop apply rate: 0.36%
TCP action: Drop apply rate: 46.15%
Other action: Drop apply rate: > 0%
Applied rules are available at the Filter wizard page for further configuration.
new analysis
apply rules

For more frequently used port numbers, a Help tooltip shows, which application is typically assigned to this port.

Rules on the overview page are even then displayed, if the action set up for the rule matches the default policy. The default policy is displayed in the filter wizard, as soon as at least one SecureNow! rule has been adopted. It defines the action which applies to all remaining packets, which so far haven't been allowed or prohibited. It is explained in more detail further below.

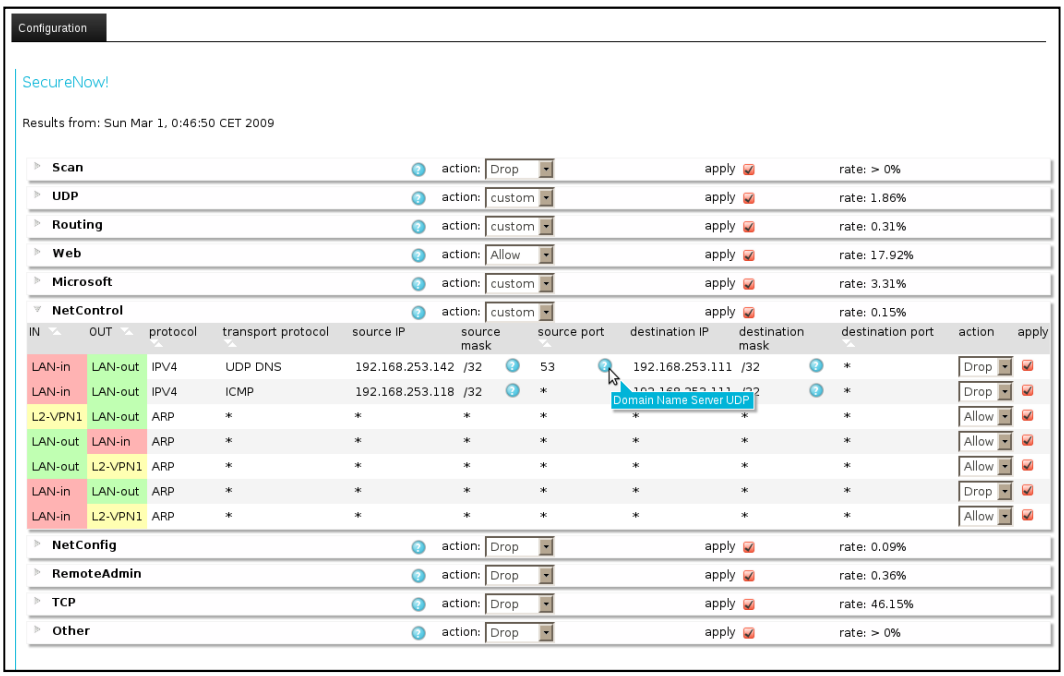
Rules, whose actions match the default policy, are actually superfluous, and it would have the same effect, for example, if only rules are adopted, which have the target action "Allow", as long as all remaining packets from the default policy are dropped. But rules with the "Drop" action are still displayed on the result page in order to give the user the opportunity of modifying the action before adopting it, if desired.

This means that in an ideal case, the entire network traffic, which passed through the firewall during the recording phase, is mapped to rules. Then there is not a single packet that doesn't match one of the displayed rules. However, there are the following exceptions:

If the traffic throughput is very high, some individual packets are not included in the analysis, i.e. they are not recorded although passing the firewall.

No separate rules are displayed for TCP packets in the return direction. In IP router mode, they are allowed by using the "def Policy rev" rule, which we will explain later. This is done by an automatic monitoring of the connection status by so-called connection tracking. In Transbridge mode, the TCP packets of the return direction are treated by using a status independent check of the TCP flags.

Packets which have been excluded from analysis by previously defined rules (later described in the "Adoption and configuration in the filter wizard" section), are not analysed and also not mapped to rules.


Configuration
SecureNow!
Results from: Sun Mar 1, 0:46:50 CET 2009
Scan action: Drop apply rate: > 0%
UDP action: custom apply rate: 1.86%
Routing action: custom apply rate: 0.31%
Web action: Allow apply rate: 17.92%
Microsoft action: custom apply rate: 3.31%
NetControl action: custom apply rate: 0.15%
IN OUT protocol transport protocol source IP source mask source port destination IP destination mask destination port action apply
LAN-in LAN-out IPV4 UDP DNS 192.168.253.142 /32 53 192.168.253.111 /32 * Drop
LAN-in LAN-out IPV4 ICMP 192.168.253.118 /32 * * Drop
L2-VPN1 LAN-out ARP * * * * * * * Allow
LAN-out LAN-in ARP * * * * * * * Allow
LAN-out L2-VPN1 ARP * * * * * * * Allow
LAN-in LAN-out ARP * * * * * * * Drop
LAN-in L2-VPN1 ARP * * * * * * * Allow
Domain Name Server UDP
NetConfig action: Drop apply rate: 0.09%
RemoteAdmin action: Drop apply rate: 0.36%
TCP action: Drop apply rate: 46.15%
Other action: Drop apply rate: > 0%

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

ADOPTION AND CONFIGURATION IN THE PACKET FILTER

A certain class, e.g. "**Industrial Ethernet**", is mapped to one or several rule sets with similar names during adoption. The rule sets are further divided regardless of which interfaces are involved in the process.

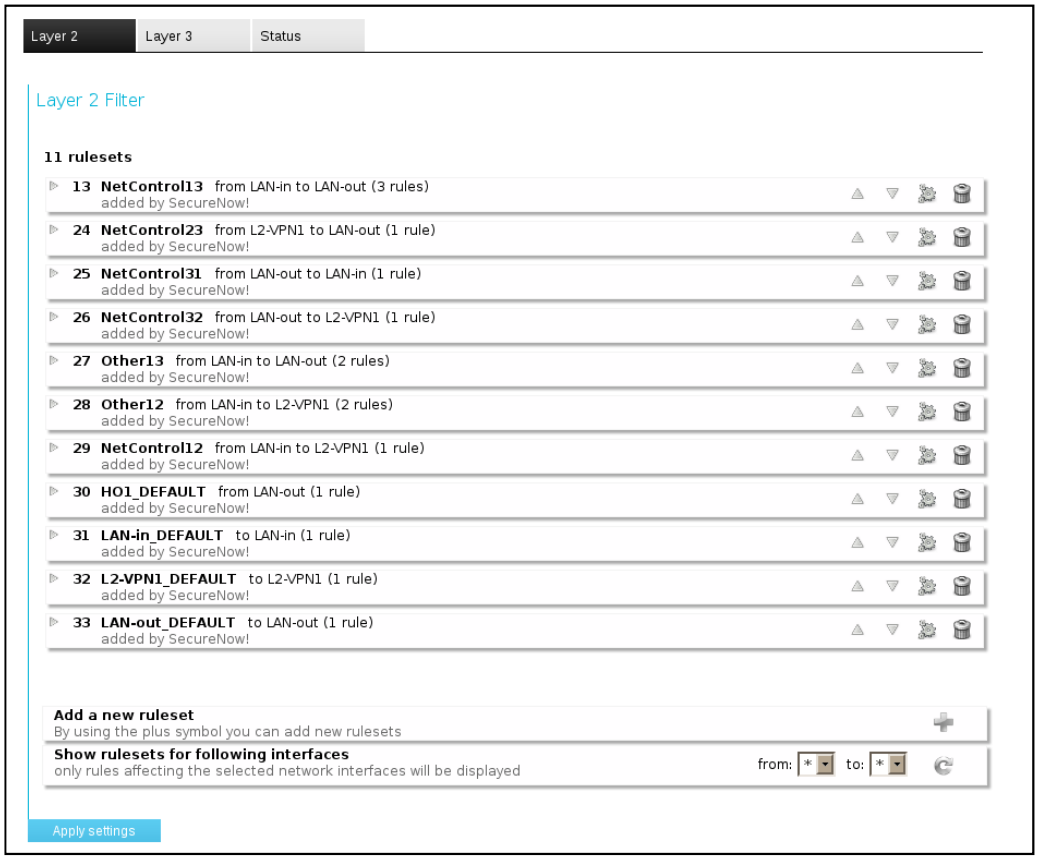
EXAMPLE:

On the result page, you can see rules under the "**Microsoft**" class, which originated from the "**Lan-out**" interface, and were directed either to the "**Lan-in**" zone or to the "**L2-VPN1**" zone. Two rule sets will be created from this in the packet filter. There will be one rule set with the traffic from **"Lan-out**" to "**Lan-in**", and another rule set for the traffic from "**Lan-out**" to "**L2-VPN1**".

Default rule sets for the different network interfaces are created in addition to the rules displayed on the result page. They define what should happen with the packets which have not been treated by any of the generated rules. These default rules are visible in the packet filter after at least one of the rules has been adopted. They can be recognised by the "**_DEFAULT**" suffix in their name, which is followed by the short ID for the corresponding interface.

The default rule sets must unconditionally be put in the last position (this happens automatically once they are adopted). But the order amongst the default rules does not matter at all.

Once automatically generated rules have been adopted in the packet filter, they are active immediately, i.e. clicking on "**Apply changes**" is no longer required.


Layer 2
Layer 3
Status
Layer 2 Filter
11 rulesets
13 NetControl13 from LAN-in to LAN-out (3 rules)
added by SecureNow!
24 NetControl23 from L2-VPN1 to LAN-out (1 rule)
added by SecureNow!
25 NetControl31 from LAN-out to LAN-in (1 rule)
added by SecureNow!
26 NetControl32 from LAN-out to L2-VPN1 (1 rule)
added by SecureNow!
27 Other13 from LAN-in to LAN-out (2 rules)
added by SecureNow!
28 Other12 from LAN-in to L2-VPN1 (2 rules)
added by SecureNow!
29 NetControl12 from LAN-in to L2-VPN1 (1 rule)
added by SecureNow!
30 HO1_DEFAULT from LAN-out (1 rule)
added by SecureNow!
31 LAN-in_DEFAULT to LAN-in (1 rule)
added by SecureNow!
32 L2-VPN1_DEFAULT to L2-VPN1 (1 rule)
added by SecureNow!
33 LAN-out_DEFAULT to LAN-out (1 rule)
added by SecureNow!
Add a new ruleset
By using the plus symbol you can add new rulesets
Show rulesets for following interfaces
only rules affecting the selected network interfaces will be displayed
from:
to:
Apply settings

Having more rules determined by SecureNow! is even possible once rules have been defined in the packet filter - regardless whether they have automatically or manually been generated. SecureNow! then generates more rules, which reasonably complement the existing ones. The network traffic matching the existing rules is then excluded from the analysis in the first place.

However, certain existing rules are not observed in the analysis:

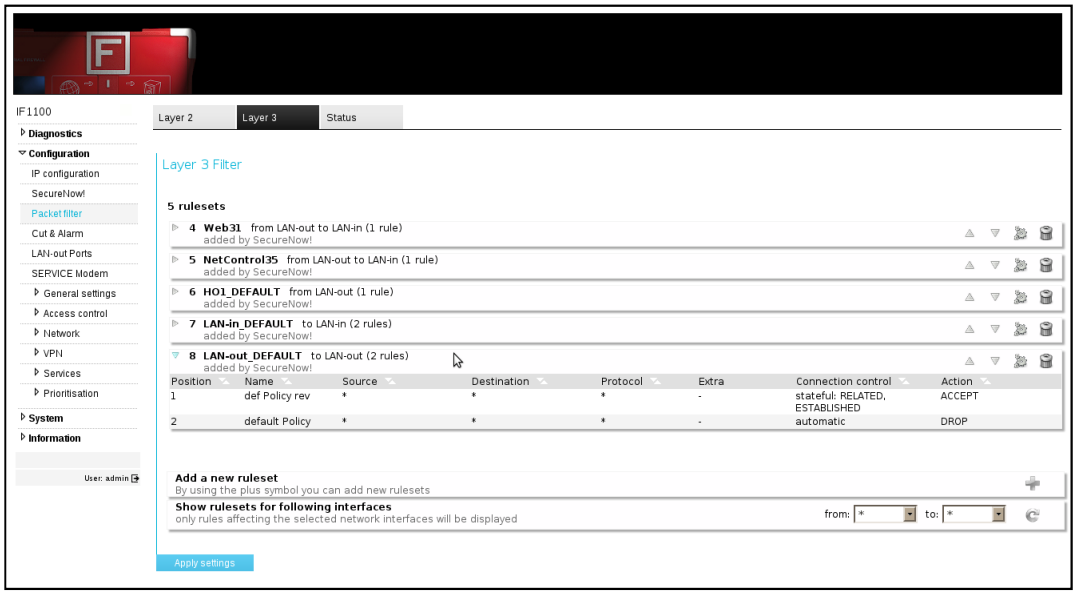
Default configuration: An "**Allow L3/L2**" rule is already included in the wizard. A default "**ARP**" rule additionally exists in Transbridge mode. SecureNow! records the traffic before it is checked by any of both rules. This means that every packet is analysed first, and only then subjected to checking with the default rules.

After completed analysis and adoption of rules: There are now several automatically generated "**_DEFAULT**" rules for every network interface in the packet filter. The network with the "low" security level forms an exception - it does not require any default rule. The mentioned "**_DEFAULT**" rules are placed in the lowest positions in the list. This allows their automatic detection in the event that SecureNow! is restarted. The network traffic, which has not yet been treated by the rules located in front of the "_DEFAULT" rules, is analysed.

Example:

There is a rule set called "**HTTP**", which prohibits HTTP. Additionally, there are two "**_DEFAULT**" rules. SecureNow! is now restarted. Every packet passing through the firewall is checked whether it meets the rule criteria in the HTTP rule set or not. The packet is dropped if this is the case - i.e. if it is HTTP traffic. All other packets are now being further treated. In this case, only the "**_DEFAULT**" rule sets are left for checking. That's why the SecureNow! analysis is first carried out at this point in time. So, all packets not considered as being HTTP are subjected to the analysis. Then the "**_DEFAULT**" rule sets are applied to the packets.

After manual configuration: If one or more "**_DEFAULT**" rule(s) generated by SecureNow! is/are in the last position(s), or if a previously defined "**Allow L2**" or "**Allow L3**" rule is in the last position, the packets are used for the SecureNow! analysis, before the corresponding default rule(s) is/are applied. Otherwise, the analysis is carried out in accordance with all existing rule sets.



© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

The two rules included in the "**_DEFAULT"** rule sets are a particularity. The rule called "**def Policy rev**" only allows packets which belong to an established TCP connection or represent responses to other packets, which have previously passed the firewall.

This rule does not exist if the firewall is operated in Transbridge mode. Extra rules are then created for the packets of the return direction.

The "**default Policy**" rule is a simple rule, which either allows or drops all inbound packets for a certain zone, depending on which security level was selected for it. If the "moderate" or "high" security level was chosen, the default policy is "**Drop**", and if the "low" security level was assigned, then the default policy is "**Allow**"/"**Accept**".

Additionally, a specific "**HO_DEFAULT**" rule is created for every security zone with a "high" security level. „**HO**" stands for "**High Out**", and the corresponding rule set includes a rule for all packets, which allows the output of all packets originating from a zone with "high" security level. This rule corresponds with the mindset that the components in the green zone are all particularly trustworthy. This rule can however be deleted, if this behaviour is undesired.

11.8 PACKET FILTER

GENERAL

Rule sets on a MAC level (layer 2) and IP level (layer 3) can be defined in order to control the data traffic through the ads-tec firewall by using the packet filter, which you can open from the start page or from the "Configuration" section. Every rule set can contain up to 10 rules, where all rules of a rule set have the same setting as far as the inbound and outbound interface is concerned. All active layer 2 rule sets are displayed on the main page of the package filter.

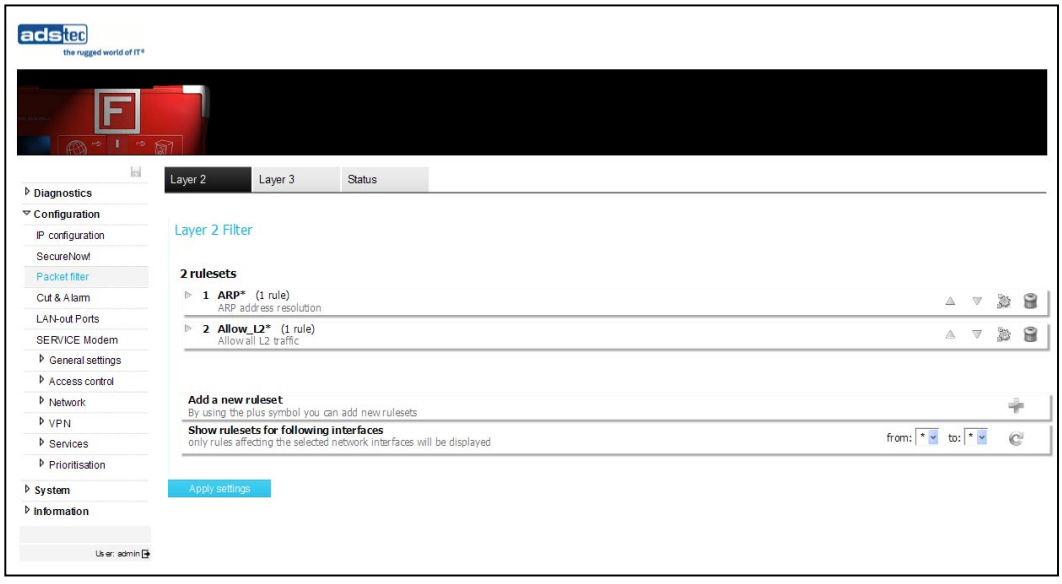
Thanks to a filter function at the bottom of the page, the displayed rule sets can be restricted by specifying the inbound and outbound interface. This has no impact on the functioning of rules: the rules not displayed are still enabled.

The toolbar for adding new rule sets is located above the filter function for the inbound and outbound interface. By clicking on the Plus icon, a dialogue window pops up, which guides the user step by step through the setup options for different protocol levels.

The overview pages for layer-2 and layer-3 rule sets are structured in the same way. All displayed rule sets can be opened by clicking on the triangular icon to the left of the rule set name, as a result of which all rules included in the set become visible.

On the right margin of the tool bar, there are the controls for modifying the position of rule sets - and of their internal order of processing, as a result - as well as an Edit and Delete icon.

An existing rule set including all rules can be modified by using the Edit icon, or a complete rule set be removed by using the Delete icon. Once a rule set is deleted in this way, it is no longer enabled, but can be re-enabled from the collection of existing rule sets by using the Plus icon on the overview page.



© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

Note:

The rule sets and the rules within the rule sets are processed from top to bottom. As soon as a packet meets the criteria of a rule, all subsequent rules of this set and the subsequent rule sets are no longer processed! This means, frequently matched rule sets and rules should be in top position in order to ensure an optimised performance!

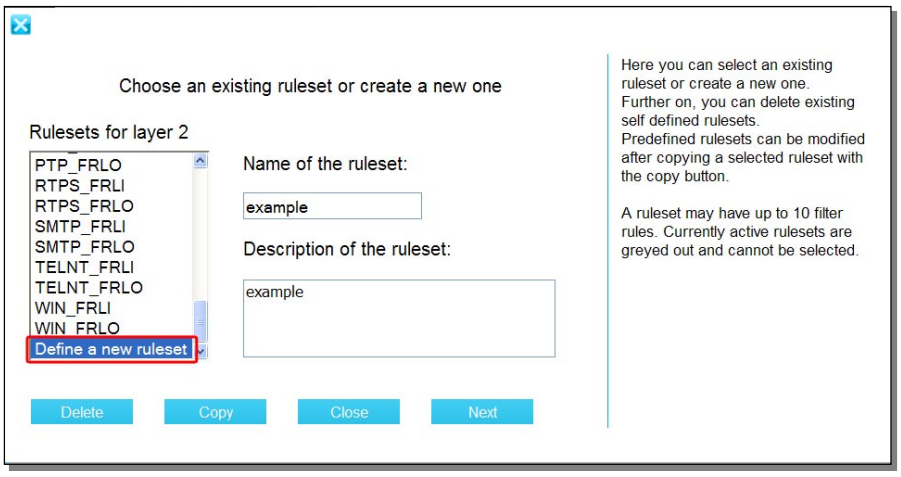
Note:

The default setting of this device is to allow all packets. Or in other words: Depending on which mode is set, and which interface is used, all Ethernet packets (layer 2) or IP packets (layer 3) are forwarded. The "Allow_L2" rule set or "Allow_L3" in the packet filter provides for that. By defining rule sets, which bar certain traffic and which are positioned in front of the "Allow_L2" / "Allow_L3" rule set in the order of processing, exceptions from this treatment can be added. They then treat the traffic like a "black list".

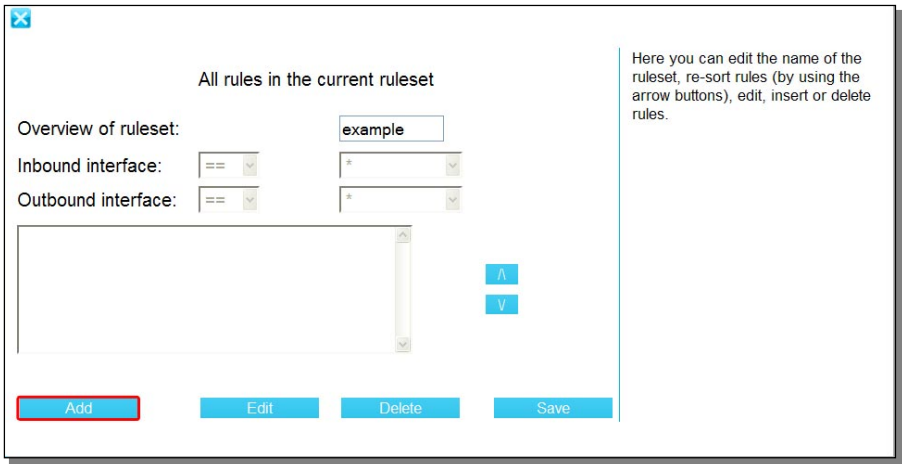
In the opposite case, traffic can be inspected by a white list, if the "Allow_L2" / "Allow_L3" rule set is deleted. Rule sets which allow certain ("white") traffic must be added in this case. Otherwise, all packets are dropped in this case, i.e. they are not forwarded.

ADDING A RULE SET FOR LAYER 2

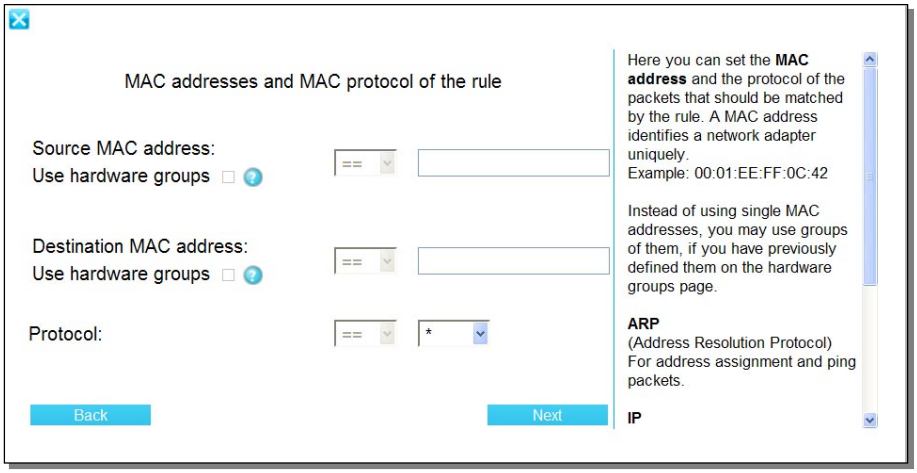
1) Select the "Define a new rule set" option in the list of existing rule sets (enabled and disabled rule sets) and give it a name as well as a short description. You can delete a rule set from the list by using the "Delete" option.


Choose an existing ruleset or create a new one
Rulesets for layer 2
PTP_FRLO
RTPS_FRLI
RTPS_FRLO
SMTP_FRLI
SMTP_FRLO
TELNT_FRLI
TELNT_FRLO
WIN_FRLI
WIN_FRLO
Define a new ruleset
Name of the ruleset:
example
Description of the ruleset:
example
Here you can select an existing ruleset or create a new one. Further on, you can delete existing self defined rulesets. Predefined rulesets can be modified after copying a selected ruleset with the copy button.
A ruleset may have up to 10 filter rules. Currently active rulesets are greyed out and cannot be selected.
Delete
Copy
Close
Next

2) Specify the traffic "direction" for the rule set: e.g. from LAN-in to LAN-out. "*" for both interfaces means that the set applies to all directions.



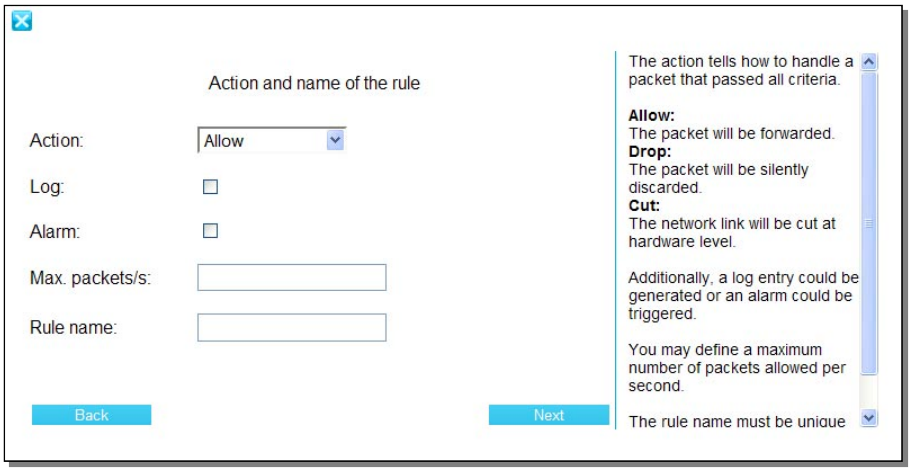
3) Then, the first rule of the rule set is directly defined. First, the source and destination MAC address (e.g. from any source to the network adapter with MAC address 00:50:c2:40:e0:aa) is specified, and then the protocol is defined for which the rule should apply. The consecutive steps for this rule then differ depending on which protocol is used. An entire group of MAC addresses can also be selected instead of a source and destination address. Hardware groups are configured in the Configuration → Network → Hardware groups menu.


MAC addresses and MAC protocol of the rule
Here you can set the MAC address and the protocol of the packets that should be matched by the rule. A MAC address identifies a network adapter uniquely.
Example: 00:01:EE:FF:0C:42
Source MAC address:
Use hardware groups
Instead of using single MAC addresses, you may use groups of them, if you have previously defined them on the hardware groups page.
Destination MAC address:
Use hardware groups
Protocol:
ARP
(Address Resolution Protocol)
For address assignment and ping packets.
Back
Next
IP

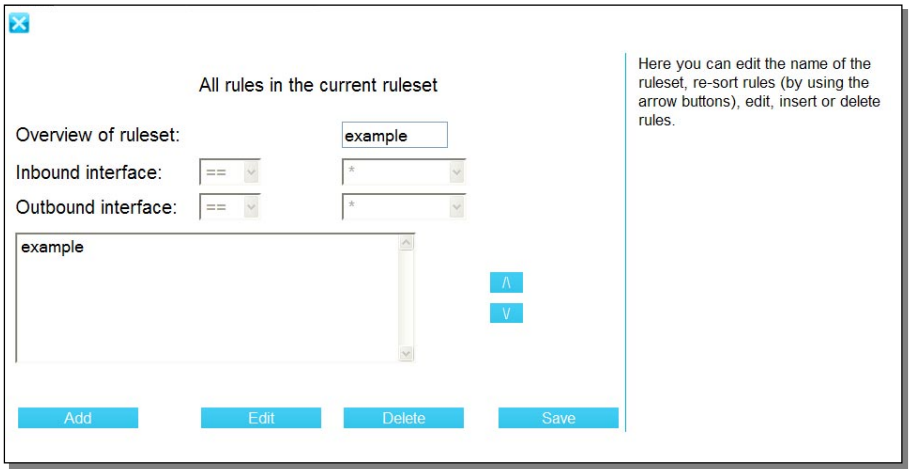
4) Depending on what was previously selected, there are protocol specific settings in this place. Refer to "Protocol specific rule settings for layer 2" further below.

5) Once the specific criteria are defined, the decision is made, what is going to happen with the packets, which meet all the criteria, as well as which name should be given to the rule within the rule set. Additionally, a log message can be generated (refer to "Structure of a log message") or an alarm can be triggered (24V are switched through to the alarm output).

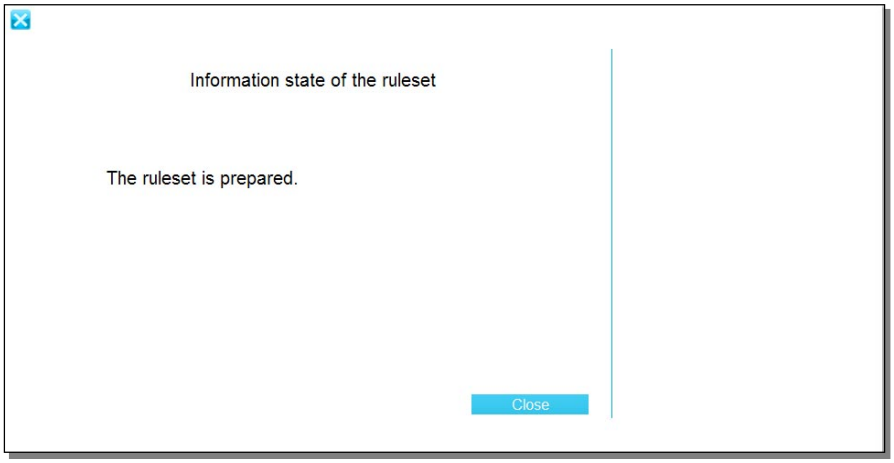
© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen


Action and name of the rule
Action:
Allow
Log:
Alarm:
Max. packets/s:
Rule name:
Back
Next
The action tells how to handle a packet that passed all criteria.
Allow:
The packet will be forwarded.
Drop:
The packet will be silently discarded.
Cut:
The network link will be cut at hardware level.
Additionally, a log entry could be generated or an alarm could be triggered.
You may define a maximum number of packets allowed per second.
The rule name must be unique

6) More rules can be added or adapted in the next step.



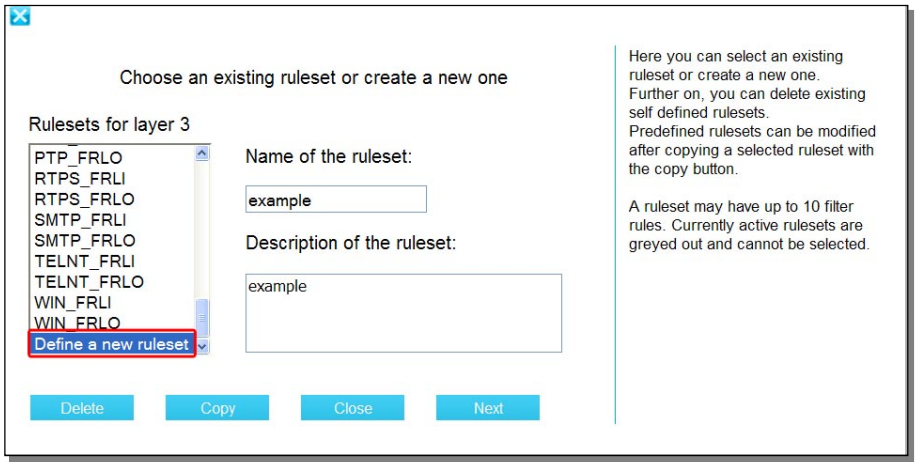
7) Finally, the rule is saved and enabled.



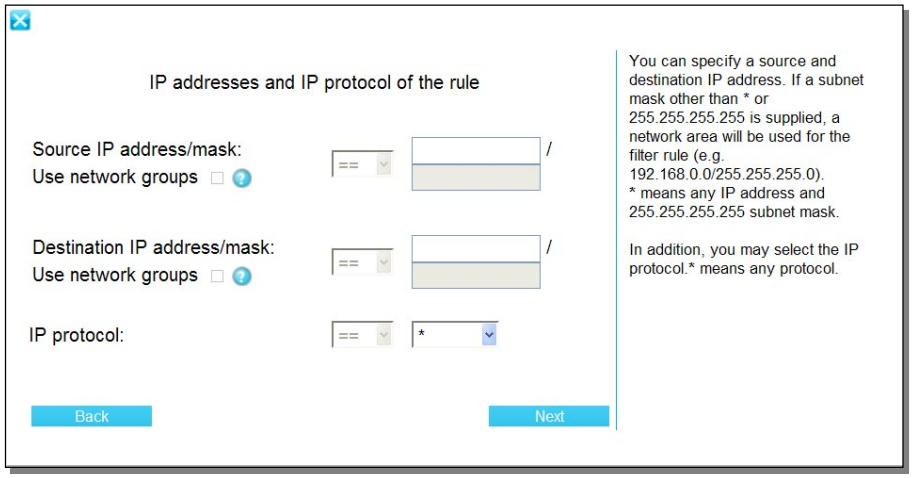
ADDING A RULE SET FOR LAYER 3

The procedure for layer 3 is the same apart from a few exceptions.

1) Only one interface, the "LAN" interface is available in Transbridge mode. Both, the inbound as well as the outbound interface must therefore be set to "*". LAN-in and LAN-out can be used for the IP router mode. The individual interfaces of LAN-out ports are additionally available in the IP router extended mode. From firmware version 2.1.0, there are additional L3 VPN interfaces available in every mode, if OpenVPN connections have previously been created with layer 3 interfaces.

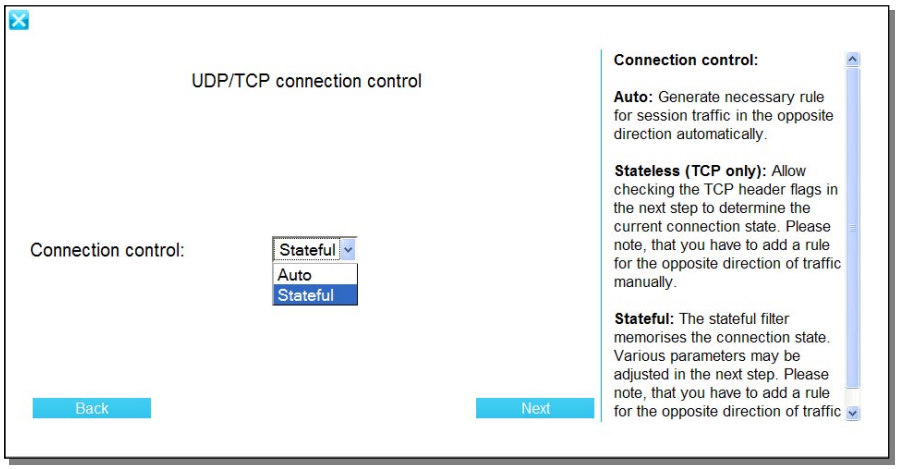

Choose an existing ruleset or create a new one
Rulesets for layer 3
PTP_FRLO
RTPS_FRLI
RTPS_FRLO
SMTP_FRLI
SMTP_FRLO
TELNT_FRLI
TELNT_FRLO
WIN_FRLI
WIN_FRLO
Define a new ruleset
Name of the ruleset:
example
Description of the ruleset:
example
Here you can select an existing ruleset or create a new one. Further on, you can delete existing self defined rulesets. Predefined rulesets can be modified after copying a selected ruleset with the copy button.
A ruleset may have up to 10 filter rules. Currently active rulesets are greyed out and cannot be selected.
Delete
Copy
Close
Next

2) IP addresses including the related subnet masks are here used instead of MAC addresses as source and destination address (e.g. from any source into the 192.168.0.1/24network). An entire group of addresses can also be selected instead of a source and destination address in this place. Network groups are configured in the Configuration → Network → Network groups menu.


IP addresses and IP protocol of the rule
Source IP address/mask:
Use network groups
Destination IP address/mask:
Use network groups
IP protocol:
==
*
/
You can specify a source and destination IP address. If a subnet mask other than * or 255.255.255.255 is supplied, a network area will be used for the filter rule (e.g. 192.168.0.0/255.255.255.0). * means any IP address and 255.255.255.255 subnet mask.
In addition, you may select the IP protocol.* means any protocol.
Back
Next

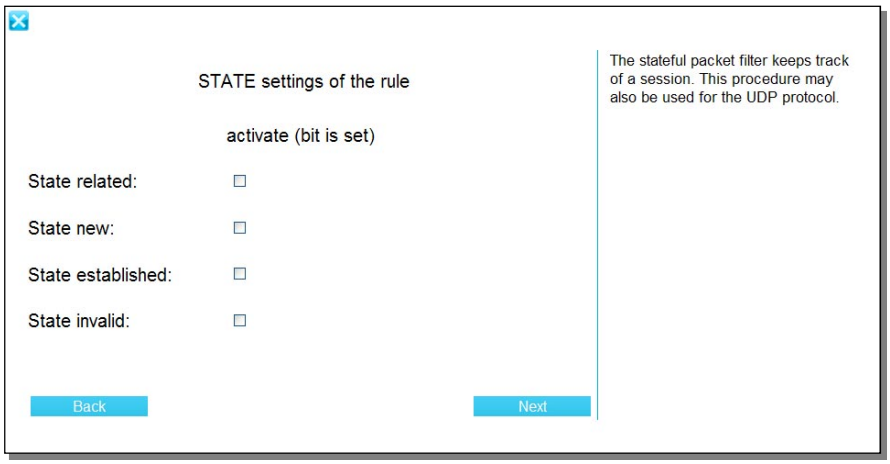
© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

3) Apart from the specific criteria which depend on the protocol used (refer to "Protocol specific rule settings for layer 3), the rule can be defined to be "stateful".

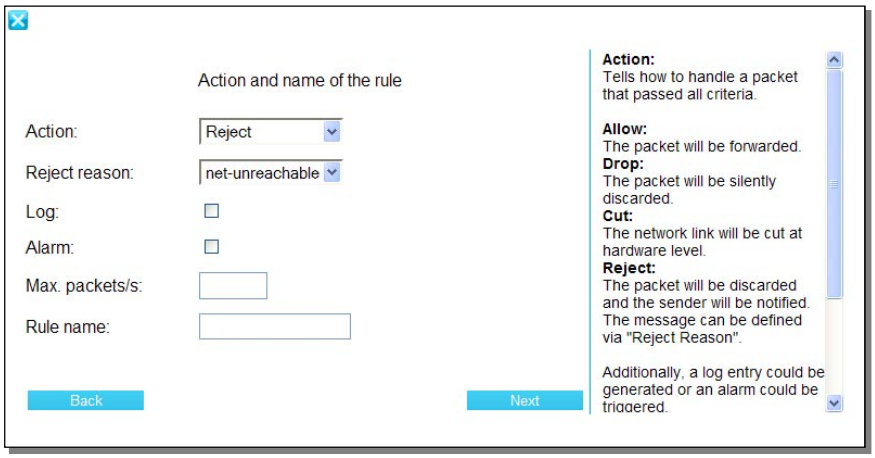

UDP/TCP connection control
Connection control:
Stateful
Auto
Stateful
Back
Next
Connection control:
Auto: Generate necessary rule for session traffic in the opposite direction automatically.
Stateless (TCP only): Allow checking the TCP header flags in the next step to determine the current connection state. Please note, that you have to add a rule for the opposite direction of traffic manually.
Stateful: The stateful filter memorises the connection state. Various parameters may be adjusted in the next step. Please note, that you have to add a rule for the opposite direction of traffic

TCP/UDP connections have extended settings - refer to the section about protocol specific settings for more information.

4) If the rule is defined to be "stateful", the firewall "memorises", which inbound and outbound packets belong to a certain TCP or UDP connection. This allows the generation of rules which depend on the corresponding connection. An example is shown in the "Port forwarding" use case.


STATE settings of the rule
activate (bit is set)
State related:
State new:
State established:
State invalid:
Back
Next
The stateful packet filter keeps track of a session. This procedure may also be used for the UDP protocol.

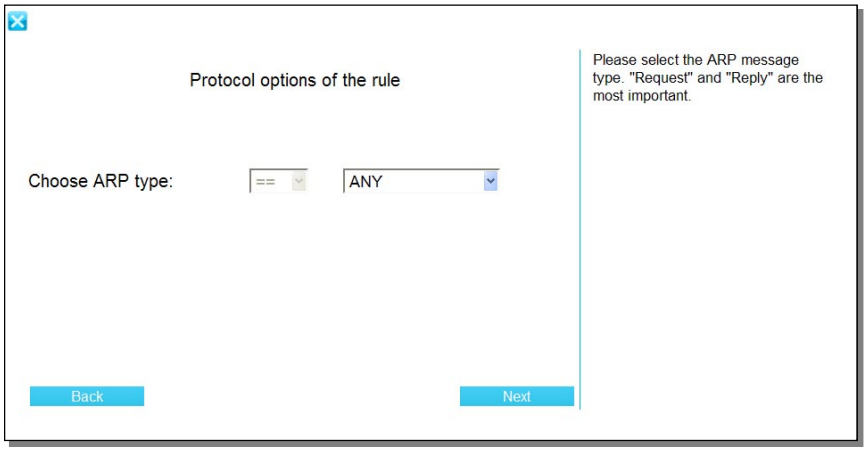
5) The additional action "Reject" exists for layer 3 for the event that all rule criteria are met. A reason can be defined for this action, which is then transmitted to the sender of this packet (via ICMP).



PROTOCOL SPECIFIC RULE SETTINGS FOR LAYER 2

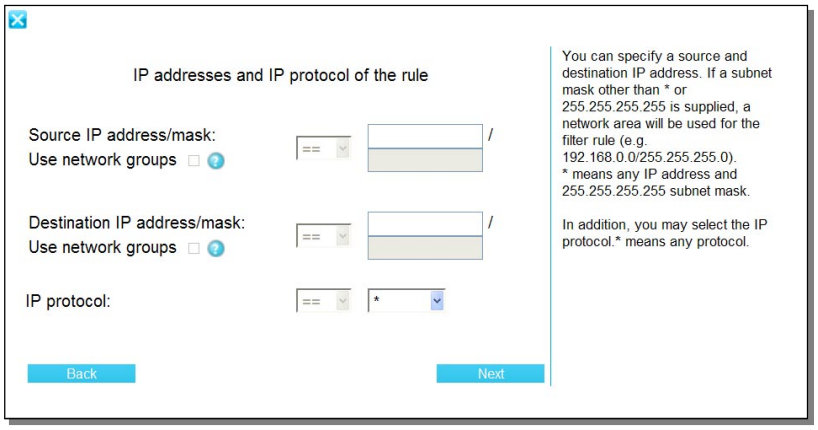
After defining the source and destination MAC address of a rule, all further steps depend on which protocol is selected.

6) ARP: The ARP type can be specified here (e.g. ANY for any type). The most important types are "Request" and "Reply", which are used for determining of IP addresses in local subnets.

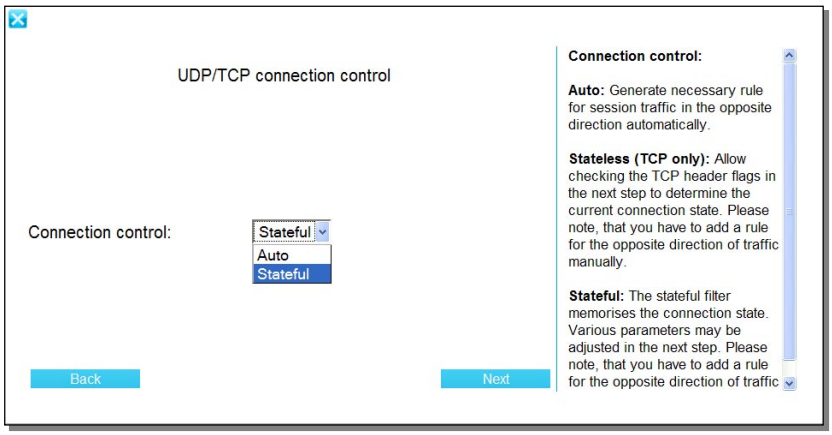


IPv4: The source address, destination address, protocol as well as (for TCP or UDP only) the source and destination port of the encapsulated IPv4 address can be verified here (the rule must e.g. apply to all TCP packets from any source which have been sent to the computer with IP address 192.168.253.162 and port number 9999). An entire group of addresses can also be selected instead of a source and destination address in this place. Network groups are configured in the *Configuration → Network → Network groups* menu.

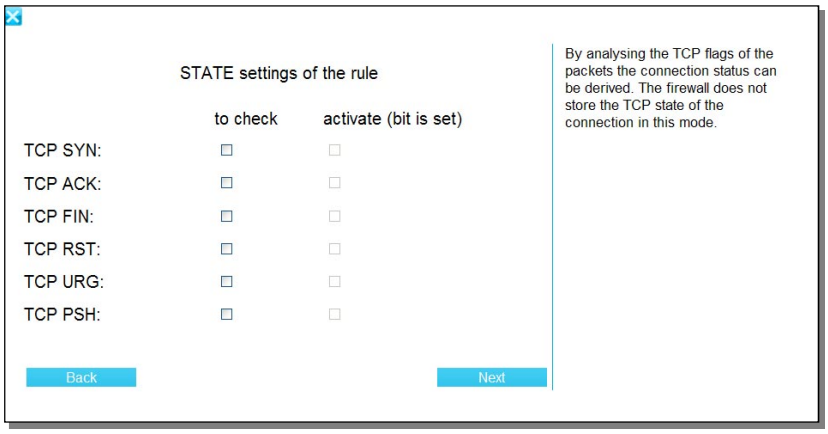
© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen


IP addresses and IP protocol of the rule
Source IP address/mask:
Use network groups
Destination IP address/mask:
Use network groups
IP protocol:
==
*
Back
Next
You can specify a source and destination IP address. If a subnet mask other than * or 255.255.255.255 is supplied, a network area will be used for the filter rule (e.g. 192.168.0.0/255.255.255.0). * means any IP address and 255.255.255.255 subnet mask.
In addition, you may select the IP protocol.* means any protocol.

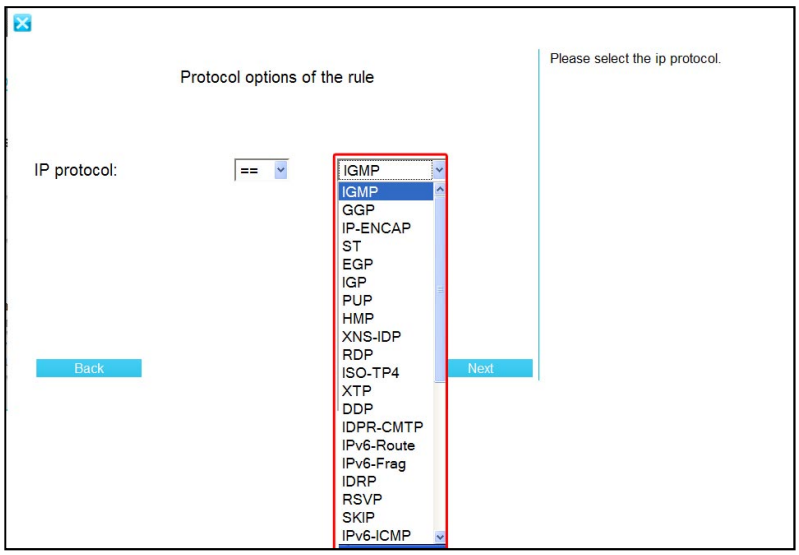
In the next step, the connection control mode can be set to "Auto" or "Manual" for the TCP or UDP protocol.


UDP/TCP connection control
Connection control:
Stateful
Auto
Stateful
Back
Next
Connection control:
Auto: Generate necessary rule for session traffic in the opposite direction automatically.
Stateless (TCP only): Allow checking the TCP header flags in the next step to determine the current connection state. Please note, that you have to add a rule for the opposite direction of traffic manually.
Stateful: The stateful filter memorises the connection state. Various parameters may be adjusted in the next step. Please note, that you have to add a rule for the opposite direction of traffic

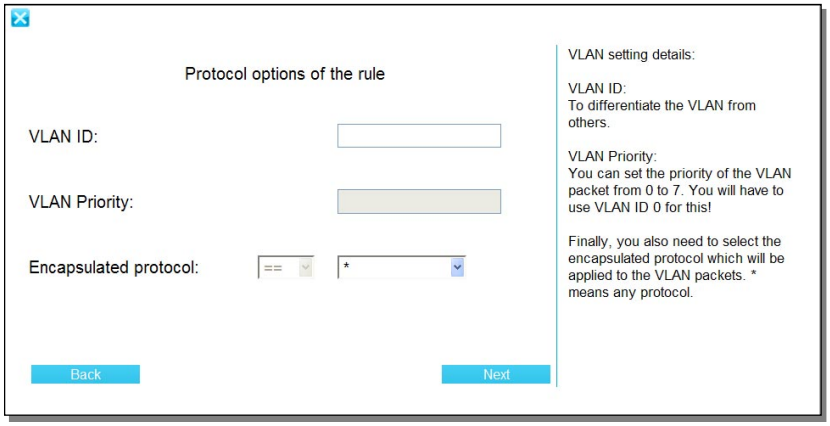
In "Auto" mode, the rules for the traffic of the same connection but in the opposite direction are automatically inserted. In "Manual" mode, the rule for the return direction must manually be defined. For the TCP protocol can then in the next step be specified, which header flags are to be checked. Which TCP flags must be checked, is defined in the "to check" column. The "Bit is set" property means that the criterion is met if the flag is set (e.g. all packets with a SYN flag, but without any ACK flag - i.e. packets which initiate a TCP connection - must meet the rule criteria).


STATE settings of the rule
to check
activate (bit is set)
TCP SYN:
TCP ACK:
TCP FIN:
TCP RST:
TCP URG:
TCP PSH:
Back
Next
By analysing the TCP flags of the packets the connection status can be derived. The firewall does not store the TCP state of the connection in this mode.

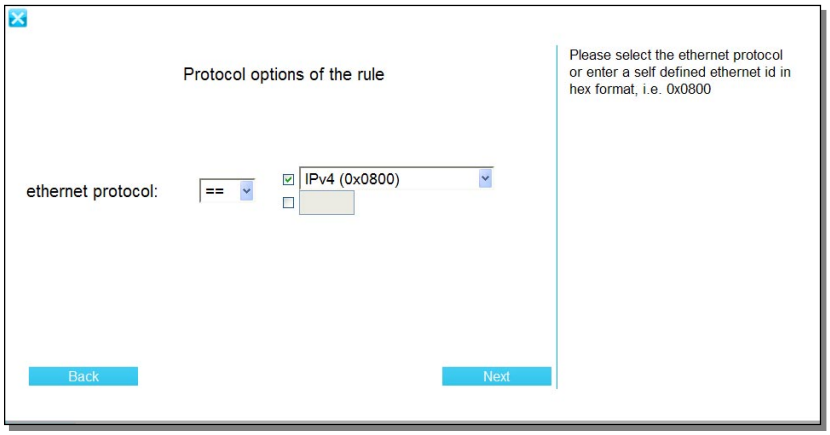
If "Other" is used as the protocol setting, you can select from an extended list of IPv4 protocols (e.g. select the PIM protocol).



7) VLAN: The 802.1Q VLAN ID of a "tagged" packet or the prioritisation level (for VLAN ID 0) and the protocol of the encapsulated packet can be checked here (e.g. IP packets tagged with ID 100 must meet the rule criteria).


Protocol options of the rule
VLAN setting details:
VLAN ID:
To differentiate the VLAN from others.
VLAN Priority:
You can set the priority of the VLAN packet from 0 to 7. You will have to use VLAN ID 0 for this!
Finally, you also need to select the encapsulated protocol which will be applied to the VLAN packets. * means any protocol.
VLAN ID:
VLAN Priority:
Encapsulated protocol:
==
*
Back
Next

8) Other: The layer 3 protocol (e.g. NetBEUI) of the packet can be specified here. If the required protocol is not available from the selection of known layer 3 protocols, you can specify a protocol number by entering the number in hex code in the bottom input box.


Protocol options of the rule
Please select the ethernet protocol or enter a self defined ethernet id in hex format, i.e. 0x0800
ethernet protocol:
==
IPv4 (0x0800)
Back
Next

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

Then, the action is specified as explained in the "Adding a rule set for layer 2" section (see further above), which is to be applied if the packet meets all criteria.

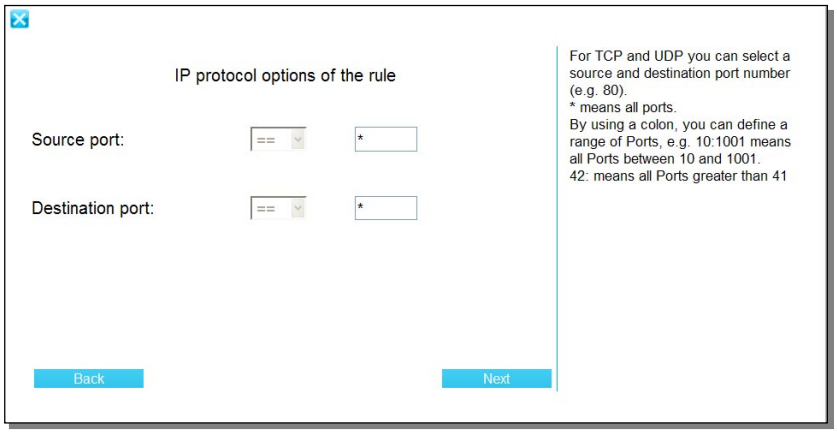
Note:

If you selected "Manual" instead of "Auto" for the connection control mode earlier, the rule for the traffic in return direction must manually be added! Please refer to the "Port forwarding" use case for a layer 3 example.

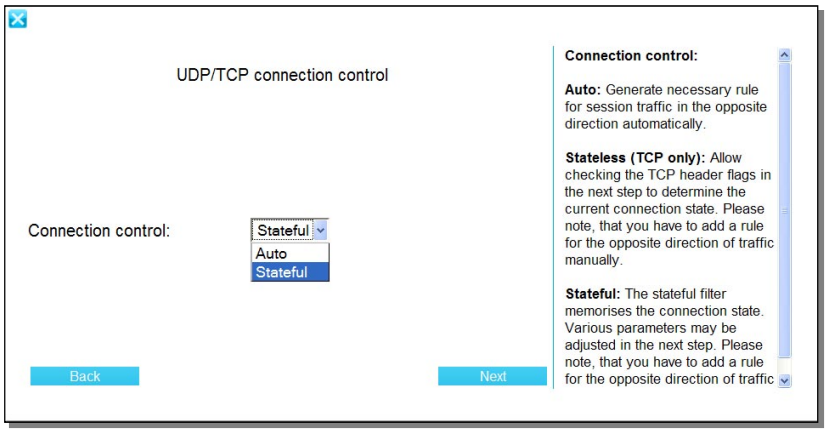
PROTOCOL SPECIFIC RULE SETTINGS FOR LAYER 3

After defining the source and destination IP address of a rule, all further steps depend on which protocol is selected.

1) TCP/UDP: Source and destination port for the packet can be specified here (e.g. from any source port to destination port 9999).


IP protocol options of the rule
Source port:
==
*
Destination port:
==
*
Back
Next
For TCP and UDP you can select a source and destination port number (e.g. 80).
* means all ports.
By using a colon, you can define a range of Ports, e.g. 10:1001 means all Ports between 10 and 1001.
42: means all Ports greater than 41

Then, the connection control mode can be set to either "Auto" or "Stateful".


UDP/TCP connection control
Connection control:
Stateful
Auto
Stateful
Back
Next
Connection control:
Auto: Generate necessary rule for session traffic in the opposite direction automatically.
Stateless (TCP only): Allow checking the TCP header flags in the next step to determine the current connection state. Please note, that you have to add a rule for the opposite direction of traffic manually.
Stateful: The stateful filter memorises the connection state. Various parameters may be adjusted in the next step. Please note, that you have to add a rule for the opposite direction of traffic

For "Auto" mode, the rule for traffic in the return direction is automatically added. For "Stateful" mode, the state settings for the connection can be set like with the other protocols. "Stateless" can additionally be used for the TCP protocol. The flags of the TCP header can be checked in this case, as described earlier in the "Protocol specific rule settings for layer 2" section.

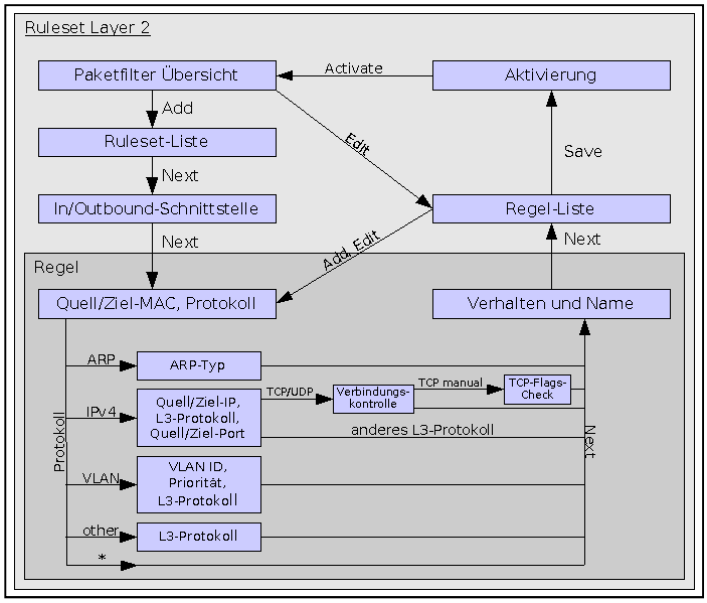
2) There are no additional options for the remaining protocols.

Then, the action is specified as explained in the "Adding a rule set for layer 3" section (see further above), which is to be applied if the packet meets all criteria.

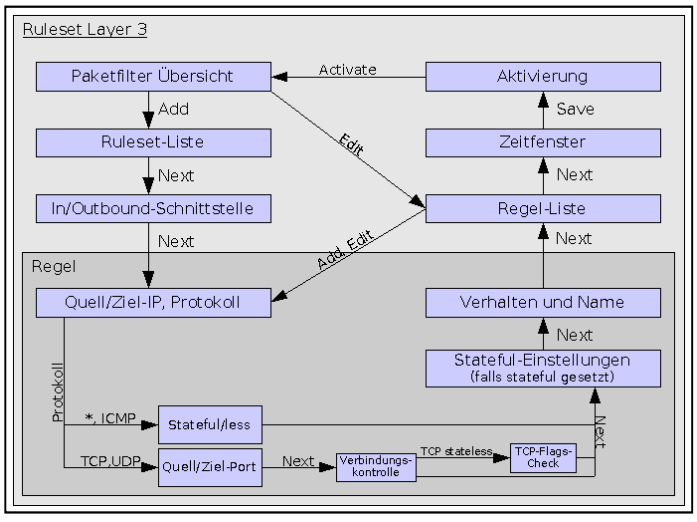
Note:

If the connection control mode for a TCP/UDP connection is not set to "Auto", the rule for the return direction must manually be added! Refer, for example, to the "Port forwarding" use case.

LAYER 2 FLOW CHART



LAYER 3 FLOW CHART



© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

EXAMPLES

The existing filter rules for layer 2 and layer 3 are good examples for the definition of your own rule sets.

STRUCTURE OF A LOG MESSAGE

If the log checkbox is ticked with a rule, and if the packet meets the criteria of this rule, the firewall generates a log entry which you can read in the "Eventlog".

If, for instance, the computer with IP address 192.168.253.161 (at the LAN-out interface) responds to a ping from the computer with the IP address 192.168.253.160 (at the LAN-in interface), if the firewall works in Transbridge mode and logs the ICMP traffic by an according rule on layer 2 level, a log entry of the form

Mar 1 02:13:13 IF-1000 kernel: icmplog.icmplogrule IN=ixp0 OUT=ixp1 MAC source = 00:50:c2:40:e0:aa MAC dest = 00:30:05:ac:b2:22 proto = 0x0800 IP SRC=192.168.253.161 IP DST=192.168.253.160, IP tos=0x00, IP proto=1

is generated, where the individual specifications have the following meanings:

icmplog.icmplogrule:	Ruleset.Rulename of the true rule
IN=ixp0	Inbound interface
OUT=ixp1	Outbound interface
MAC source = 00:50:c2:40:e0:aa	MAC address of the source adapter
MAC dest = 00:30:05:ac:b2:22	MAC address of the destination adapter
proto = 0x0800	Ethernet protocol (here IP)
IP SRC=192.168.253.161	IP address of the source computer
IP DST=192.168.253.160	IP address of the destination computer
IP tos=0x00	Type of service
IP proto=1	IP protocol (here ICMP)

If the firewall works in router mode (LAN-in IP address 192.168.172.162, LAN-out IP address 192.168.253.162), and if the computer with IP address 192.168.172.219 (at the LAN-in interface) sends a ping request to the computer with IP address 192.168.253.161 (at the LAN-out interface), if the firewall logs the ICMP traffic on layer 3, then the following entry is for instance generated:

Mar 1 03:00:06 IF-1000 kernel: icmplog3.icmplog3rule IN=ixp1 OUT=br0 PHYSOUT=ixp0 SRC=192.168.172.219 DST=192.168.253.161 LEN=84 TOS=0x00 PREC=0x00 TTL=63 ID=0 DF PROTO=ICMP TYPE=8 CODE=0 ID=20769 SEQ=11

The individual specifications have the following meaning:

icmplog3.icmplog3rule	Ruleset.Rulename of the true rule
IN=ixp1	Inbound interface
OUT=br0	Outbound interface (br0 corresponds to ixp0)
PHYSOUT=ixp0	Outbound interface
SRC=192.168.172.219	Source IP address
DST=192.168.253.161	Destination IP address
LEN=84	Packet size
TOS=0x00	Type of service
PREC=0x00	(For internal use)
TTL=63	Time to live
ID=0	(For internal use)
DF	(for internal use)
PROTO=ICMP	IP protocol
TYPE=8	Sub type (here request)
CODE=0	(For internal use)
ID=20769	ID of this connection
SEQ=11	Sequential number of the current packet

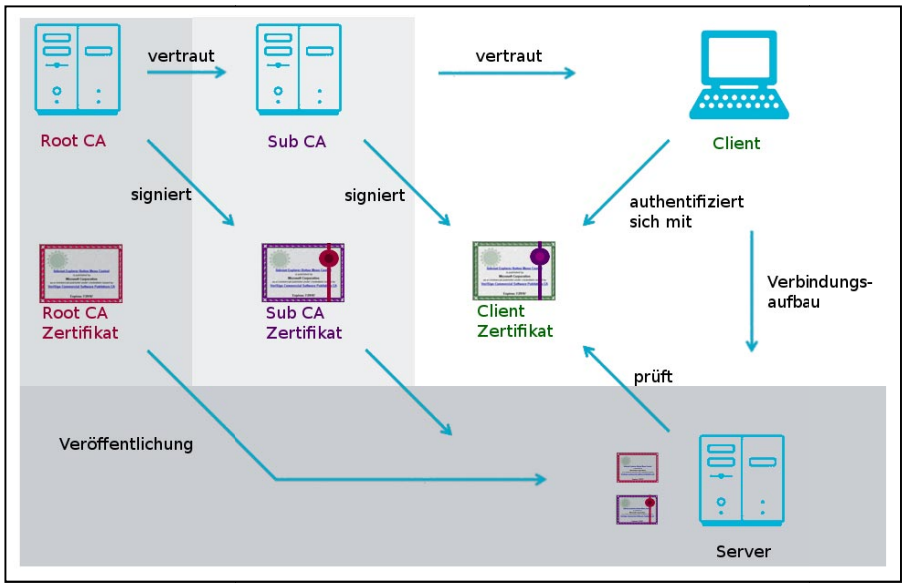
© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

11.9 CERTIFICATES

GENERAL

Certificates are used for authentication of computers or users, as well as for encryption of connections (e.g. OpenVPN, IPsec, websites). The certificate must have been signed by a certification authority (CA) so that it can be used for this purpose. For authentication the remote terminal certificate is verified with the CA certificate. The remote terminal is authenticated if the signature is valid and the CA is trustworthy. The CA certificate is also called root certificate, if it is the basis (root) for authentication, and has not been signed by another instance (self-signed certificate). Such a root CA can then be used for signing other, subordinate CA certificates. A chain of trust is built in this way, with the root certificate being the root of it.

The certificates of all superior CAs must be available if a certificate is to be signed, which was signed by a CA not identical with the root CA.



Example: A root CA (ads-tec Root-CA) signs a subordinate sub CA (ads-tec ST-CA), which in turn signs the client certificate for an OpenVPN connection. Both the certificate of "ads-tec ST-CA", as well as the certificate of "ads-tec Root-CA", must be available on the system in order to verify the client certificate.

ads-tec Industrial Firewalls support these multi-level CA hierarchies. As long as all CA certificates of the hierarchy are available, the complete hierarchy paths are always checked with certificate based services (e.g. OpenVPN, IPsec, Radius). Should one CA certificate of the chain turn out to be invalid, then all subordinate certificates are considered as invalid as well.

In order to prevent any misuse of lost or compromised certificates, a Certificate Revocation List (CRL) may be created by the CA. Certificates on this list will then be invalid despite a correct signature.

Note:
With this authentication method it will be verified if a certificate has been issued (or signed) by a certain certification authority. In this case, security is based on trusting the

certification authority, i.e. on the trust in the fact that this authority has issued (or signed) the certificate for the specified purpose (e.g. for authentication of a certain website) only!

CREATING CERTIFICATES WITH OPENSSL

CA certificates and thus also signed certificates can be created with OpenSSL via prompts. You can download OpenSSL for Windows from http://www.openssl.org/related/binaries.html . You'll find instructions e.g. on:

- http://www.online-tutorials.net/security/openvpn-tutorial/tutorials-t-69-209.html
- http://www.madboa.com/geek/openssl/



Note:

Exemplary certificates are used for illustration only, and may under no circumstances be used for a genuine authentication!

Certificates are valid from the date and time of their creation - the date on the computer used for creating them therefore must be correct.

You can also create a certificate infrastructure by using Microsoft Windows Server 2000/2003 PKI. A starting point would be: http://www.microsoft.com/pki.

Identity data (country name, etc.) must be indicated in order to make all certificates unique! Two different certificates must never use exactly the same data. At least one field must differ (for instance Common name).

Certificate administration with OpenSSL is somewhat cumbersome due to the laborious Windows command line control, which is why we recommend using a graphical frontend instead for all use cases of a smaller scale. In the next chapter, we therefore explain how to use the free "XCA" software for this purpose.

CREATING CERTIFICATES WITH XCA

Key administration with XCA for OpenVPN

This chapter explains how you can create and control CA, server and client certificates with XCA - specifically for the use with OpenVPN.

Introduction:

XCA is a very useful and versatile tool for managing certificates. The variety of options can be a little bit confusing at the start, if you'd "only" like to create a few certificates for OpenVPN. This document is based on version 0.9.0 of the XCA software.

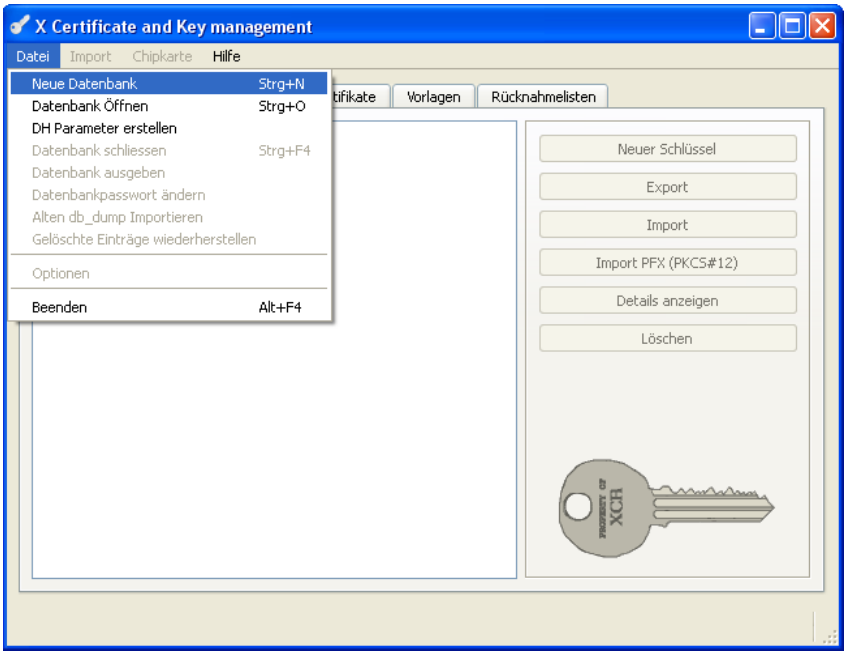
© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

Helpful links:

You'll find some additional hints and tips at: http://XCA.sourceforge.net/

The current version of the XCA software can be downloaded from: http://sourceforge.net/projects/XCA/

Please install the programme and adopt the default settings in the basic setup. After the initial programme start, you'll create a new database:

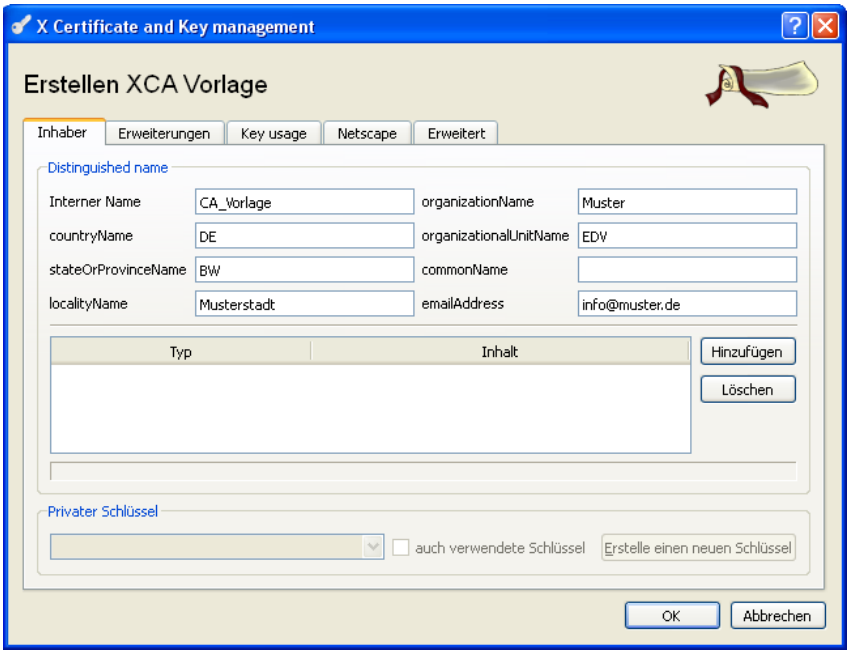


Use a plausible name like "**CA_Projectname**". This database must be encrypted with a password: Preserve the password well!

In preparation, you should create templates for the 3 default work steps in order to simplify the use of XCA for yourself right from the start.

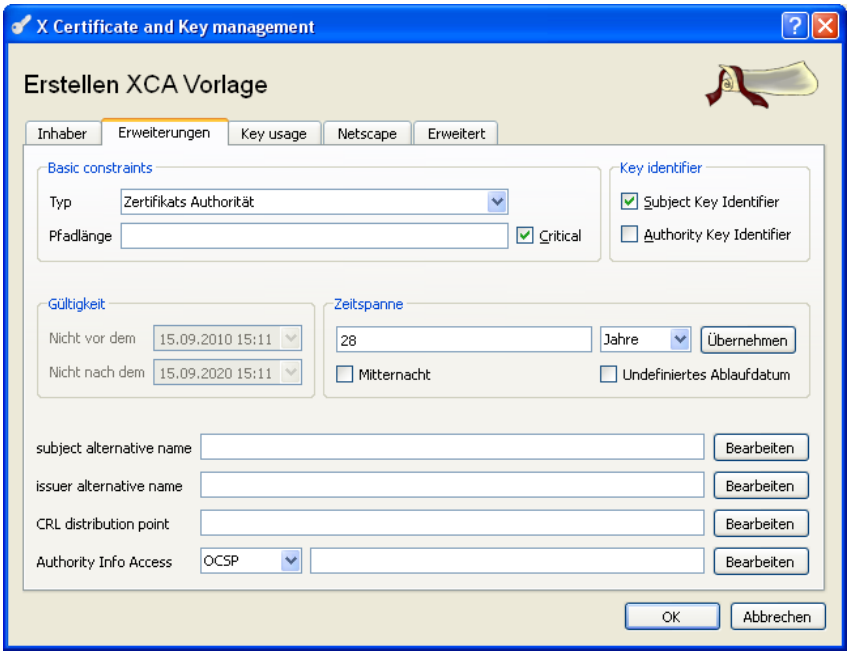
Go to the "**Templates**" tab, select there "**New template**" and then select "**CA**" in the pop up window, which appears next.

Enter "**CA_template**" as the "**Internal name**" for this new CA template. Fill all boxes except for "**commonName**". This box has to remain blank.



In the next tab called "**Advanced**", the standard validity period for certificates can be set up.

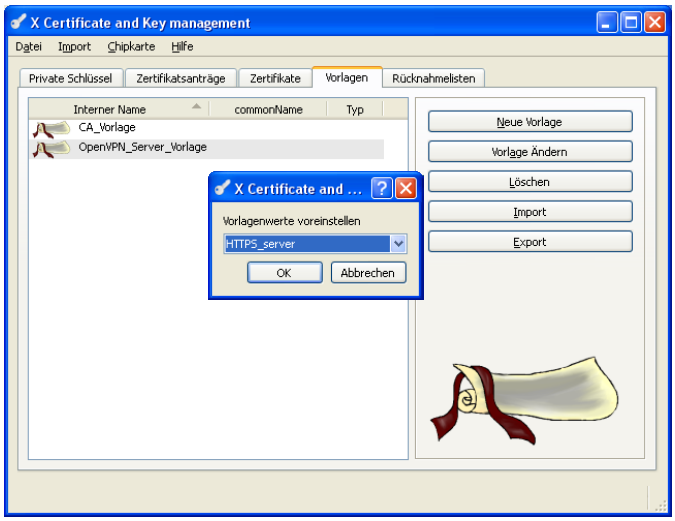
Selecting a long period of time here is usually recommended.



Once you click now on "**OK**", you should get a message that your CA template has successfully been created.

Repeat all previous steps but select now "**HTTPS_server**" as a template.

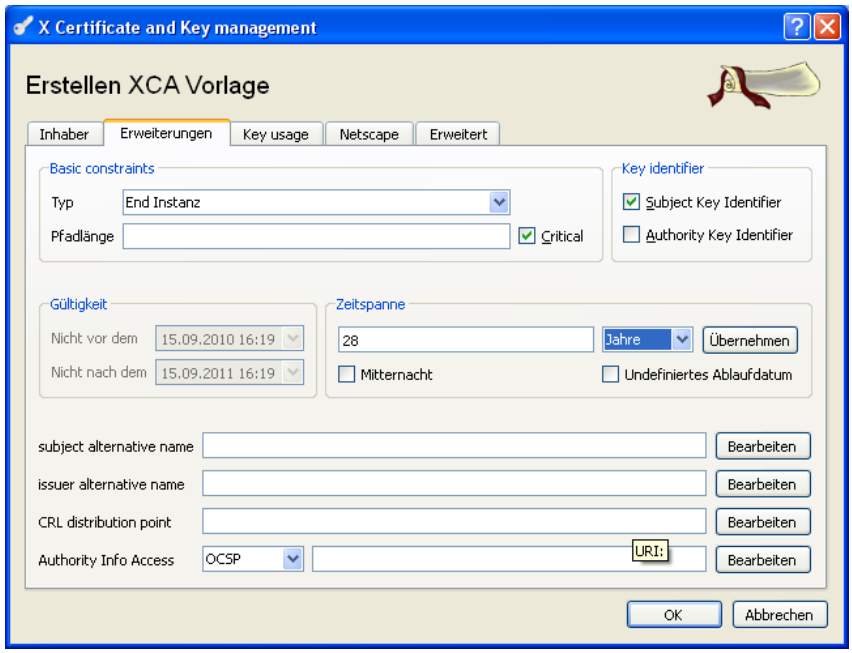
© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen



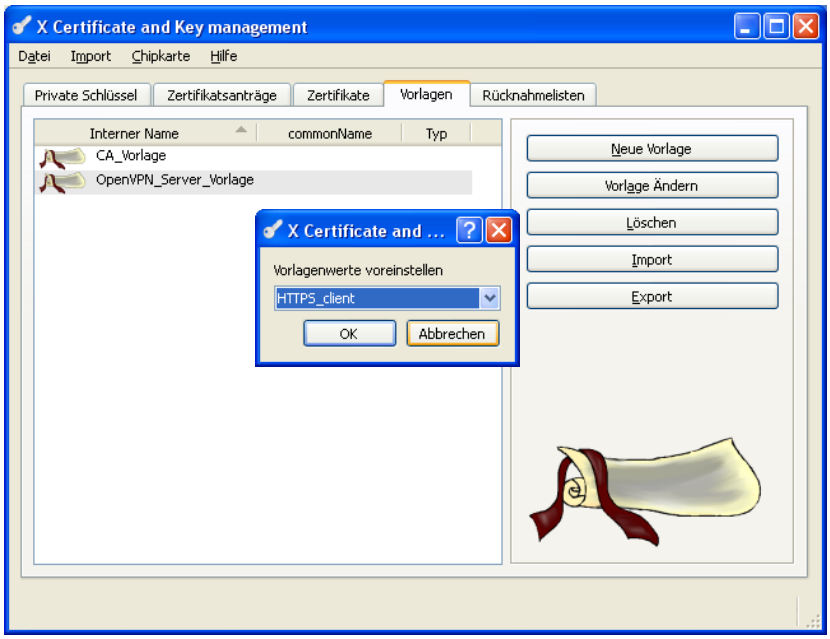
For the "**Internal name**", we recommend using "**OpenVPN_Server_Template**". All other values should remain like in the CA template.

Please pay particular attention to the validity period of certificates. It can be useful to renew a certificate after a certain period of time and therefore to select a shorter validity period, under certain circumstances.

Otherwise, you should select a longer period of time:

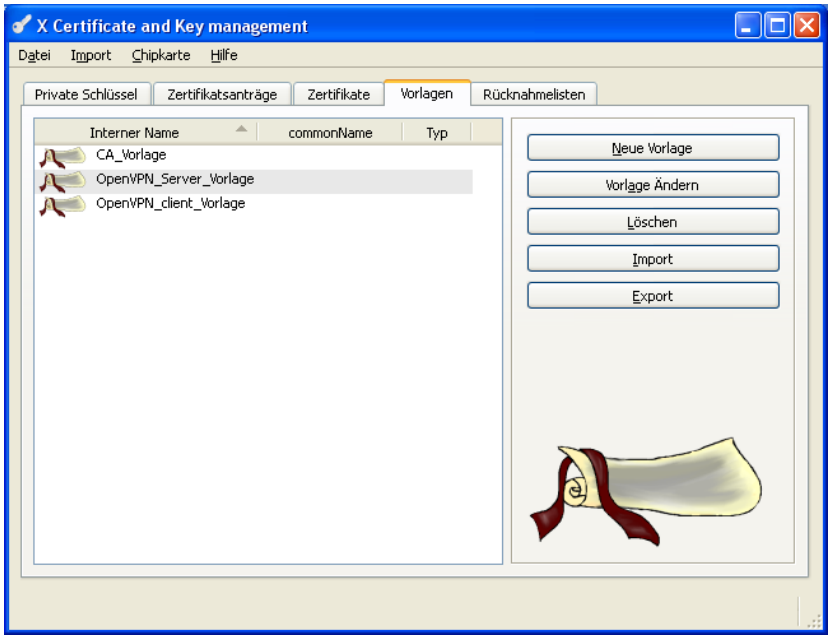


The third and last step in this process is creating the "**HTTPS_client**" template.



For the "**Internal name**", we recommend using "**OpenVPN_client_template**", for example. Otherwise, please select the same values as with the server and CA template.

The following three templates should be present now:

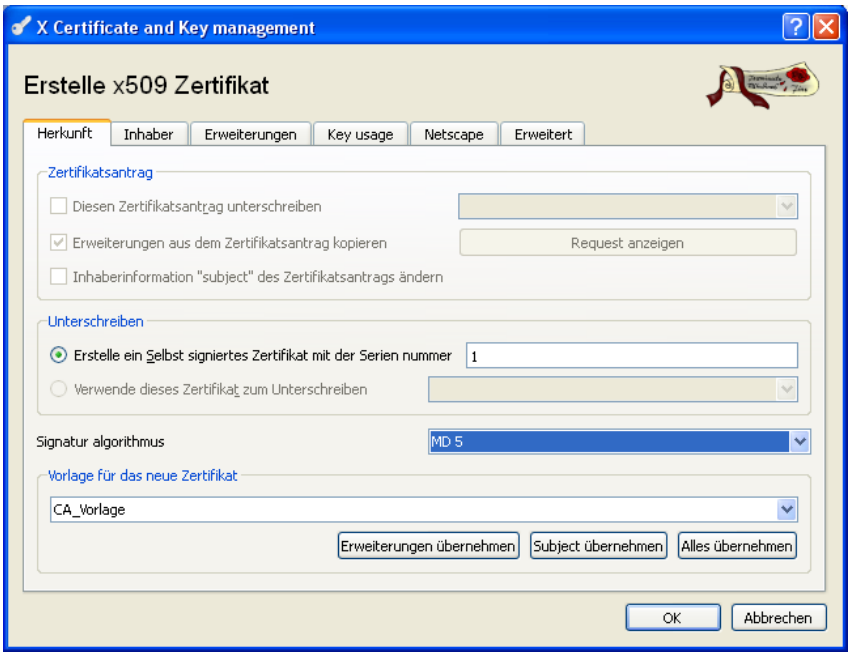


CREATING A CA

Now, you can start creating the required files. You can now use the previously created CA template for creating a CA. Select the "**Certificates**" tab, and then "**New certificate**". Now, select your CA template ("CA_template") in the new window, in the "**Origin**" tab.

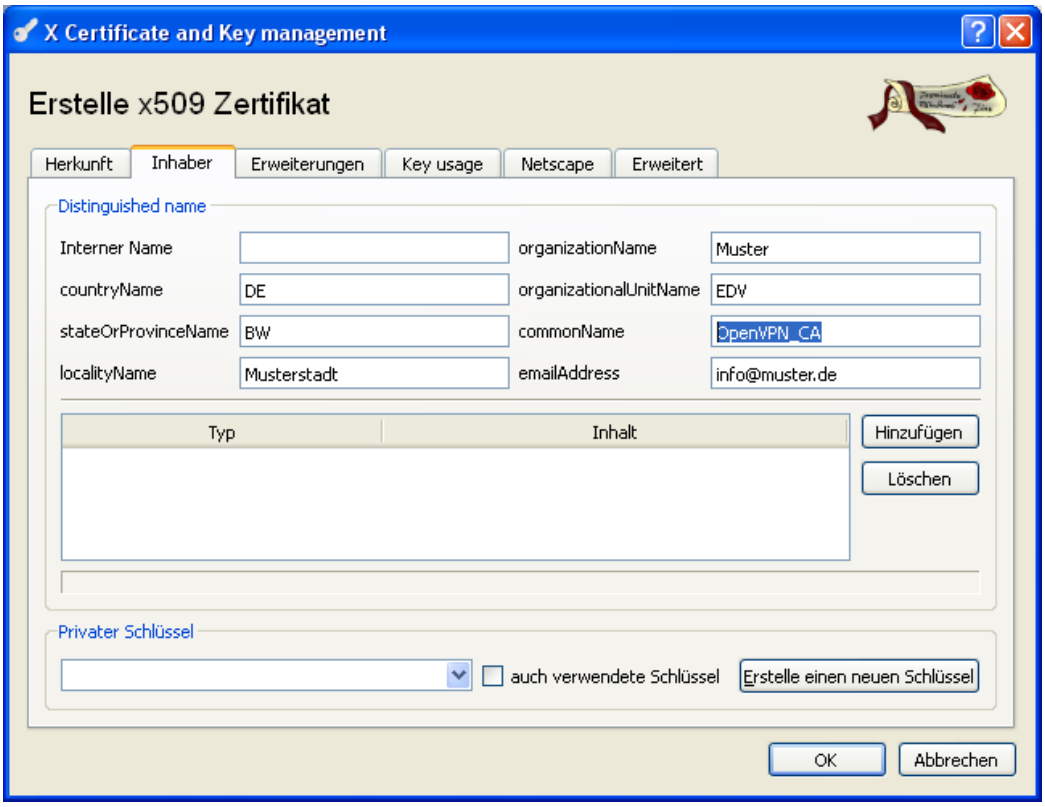
© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

Go into the "**Signature algorithm**" field and switch to **'MD5'**. **Please don't forget to push the "Save all" button in order to confirm your settings.**

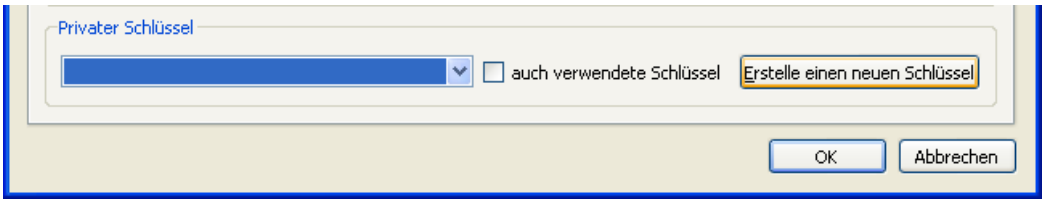


Enter a name, e.g. OpenVPN_CA in the next tab called "**Owner**", in the "**commonName**" box.

All remaining boxes should have been filled automatically with the values from your template.

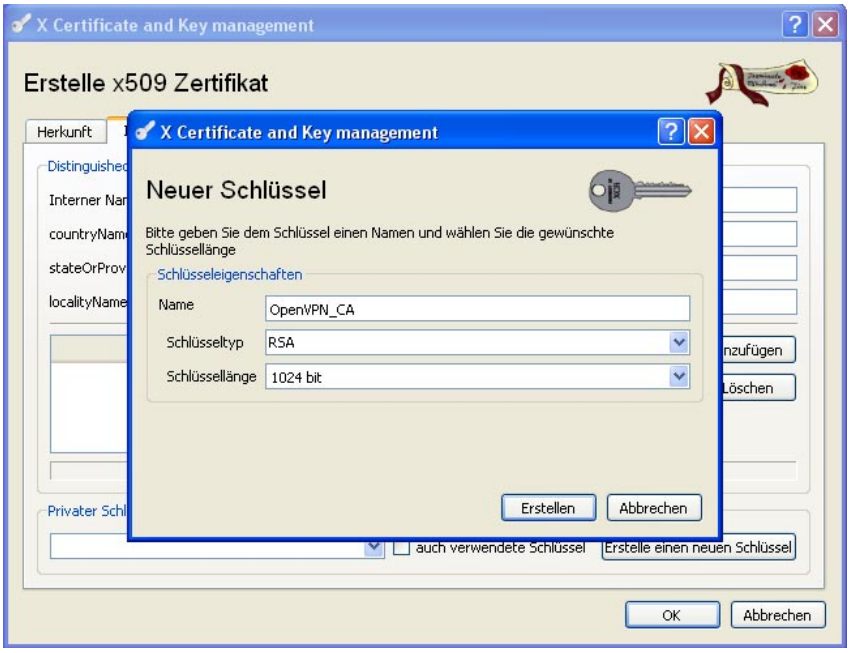


Then click on "**Create a new key**". The best idea is to use the same name in this place as you've used in "**commonName**". That means in our example: „**OpenVPN_CA**".

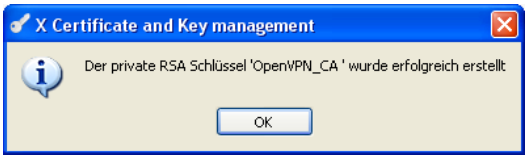


You should adapt the length of the key in accordance with your security demands. It has to be considered though, that long keys will reduce the VPN speed and increase the loading time for the Industrial Firewall operating system.

The setting "**2048 bit**" is usually a good choice, which also provides high security at the same time.



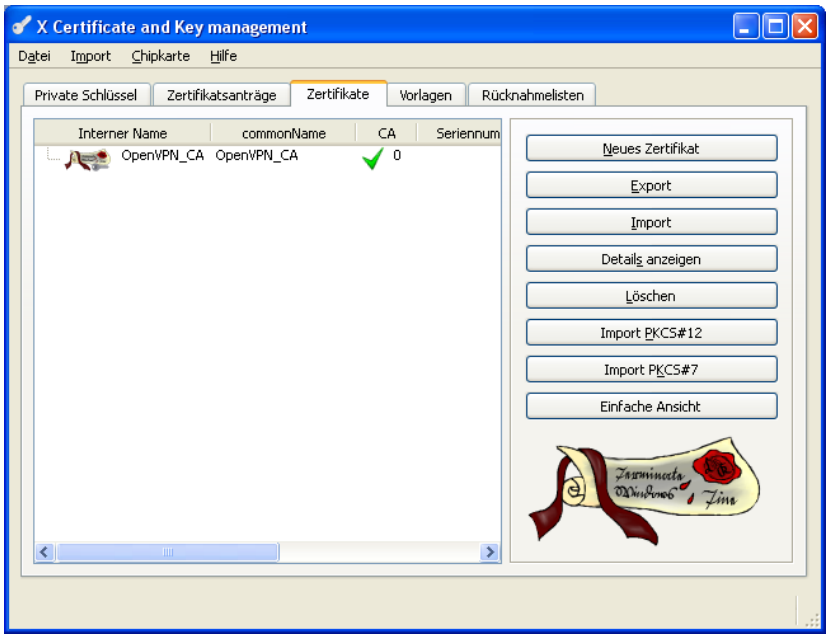
Now click on "**Create**". The following message should appear:



© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

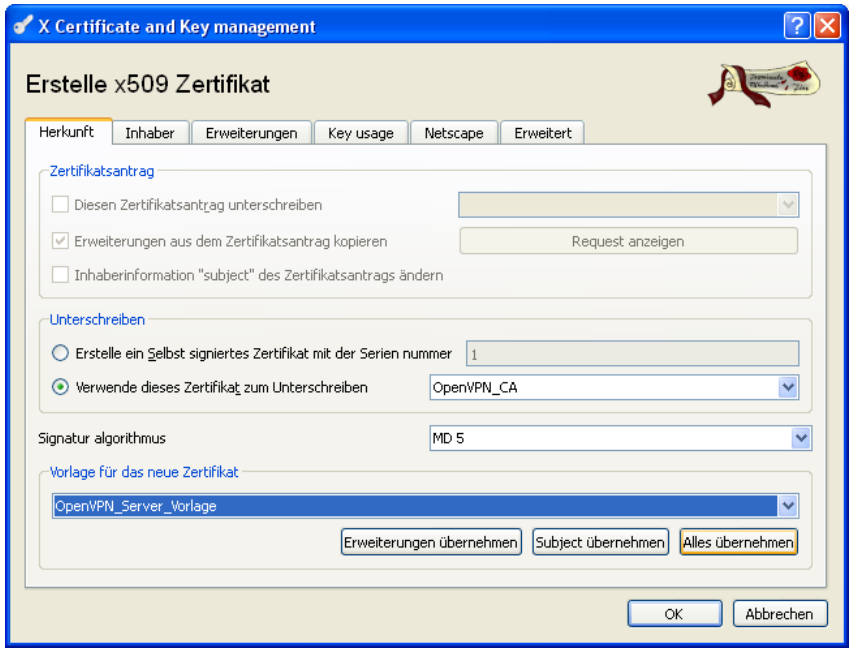
CREATING A SERVER CERTIFICATE

Once again, select "**New certificate**".



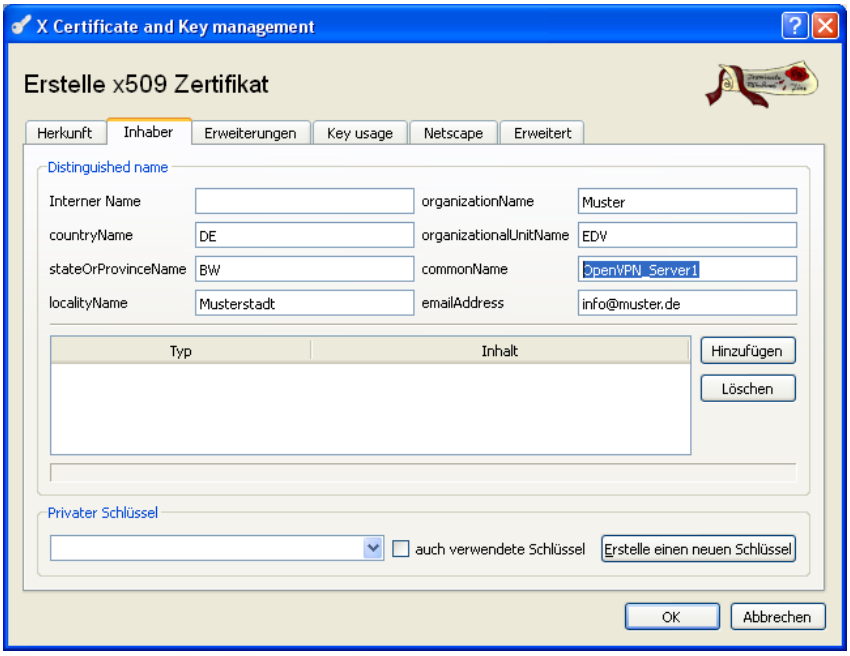
For the "**Signature algorithm**", please select **'MD5'**. Go to the "**Signature**" section and switch to "**Use this certificate as a signature**" and select the CA you've just created before.

This time, the server template created at the start is used as a template. Please don't forget to click on **"Save all"** at the end!


X Certificate and Key management
Erstelle x509 Zertifikat
Herkunft Inhaber Erweiterungen Key usage Netscape Erweitert
Zertifikatsantrag
Diesen Zertifikatsantrag unterschreiben
Erweiterungen aus dem Zertifikatsantrag kopieren
Request anzeigen
Inhaberinformation "subject" des Zertifikatsantrags ändern
Unterschreiben
Erstelle ein Selbst signiertes Zertifikat mit der Serien nummer 1
Verwende dieses Zertifikat zum Unterschreiben OpenVPN_CA
Signatur algorithmus MD 5
Vorlage für das neue Zertifikat
OpenVPN_Server_Vorlage
Erweiterungen übernehmen Subject übernehmen Alles übernehmen
OK Abbrechen

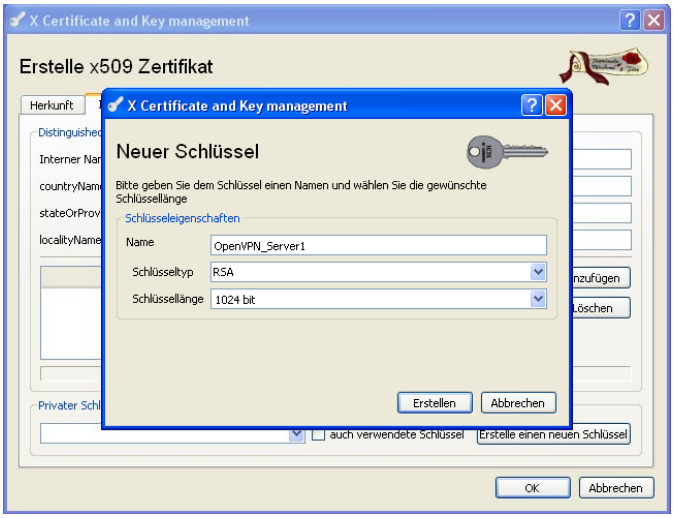
Switch to the "**Owner**" tab and enter a name in the "**commonName**" box, for instance: "**OpenVPN_Server1**".

All remaining boxes should have been filled automatically with the values from your template.



All that's left to do for you now, is to create a new key for this certificate.

Go to the **"Create a new key"** section and enter the same name as used in the "**commonName**" box for this certificate.

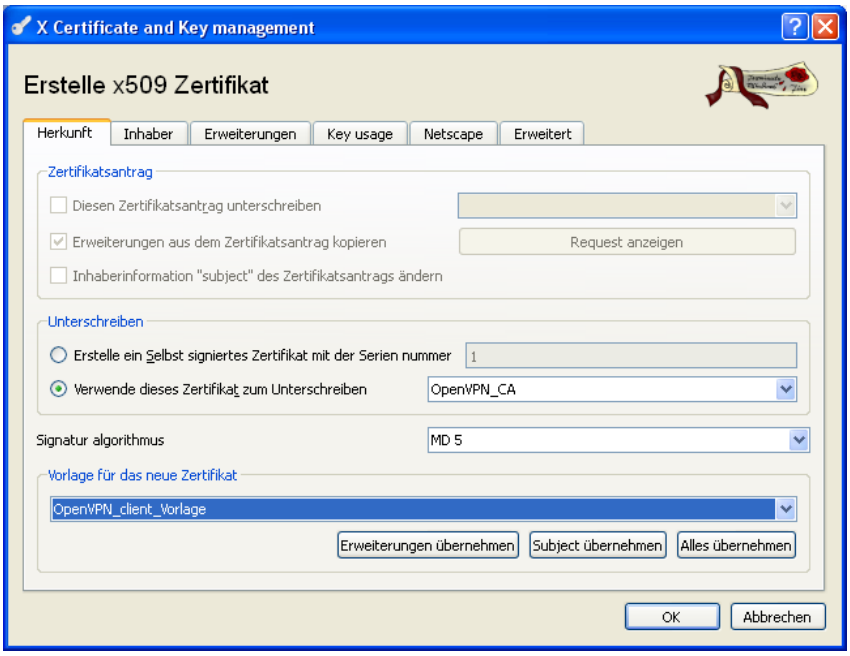


© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

CREATING A CLIENT CERTIFICATE

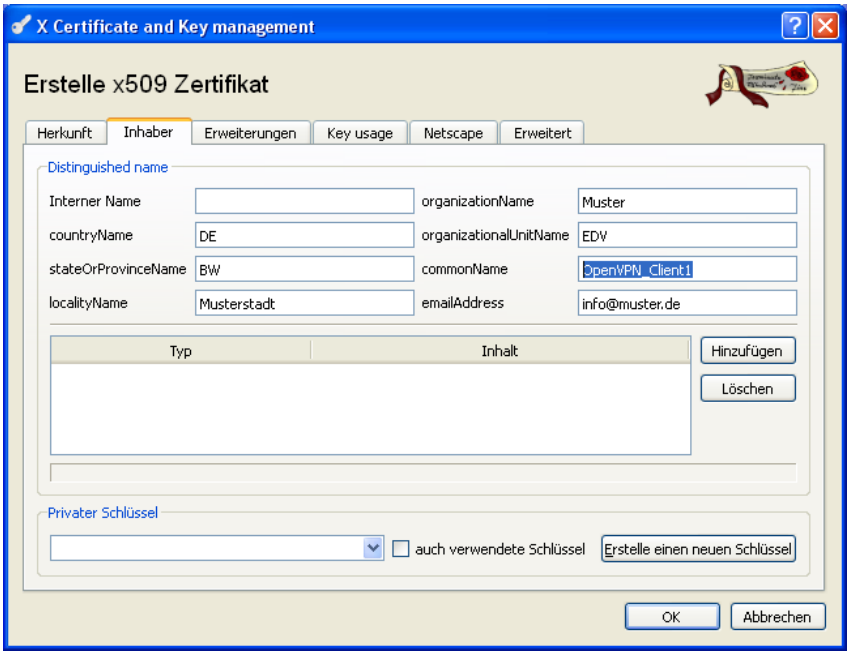
A new individual certificate must be created for every client.

Repeat the steps from the server certificate creation, but select the previously created "**Client template**", this time.

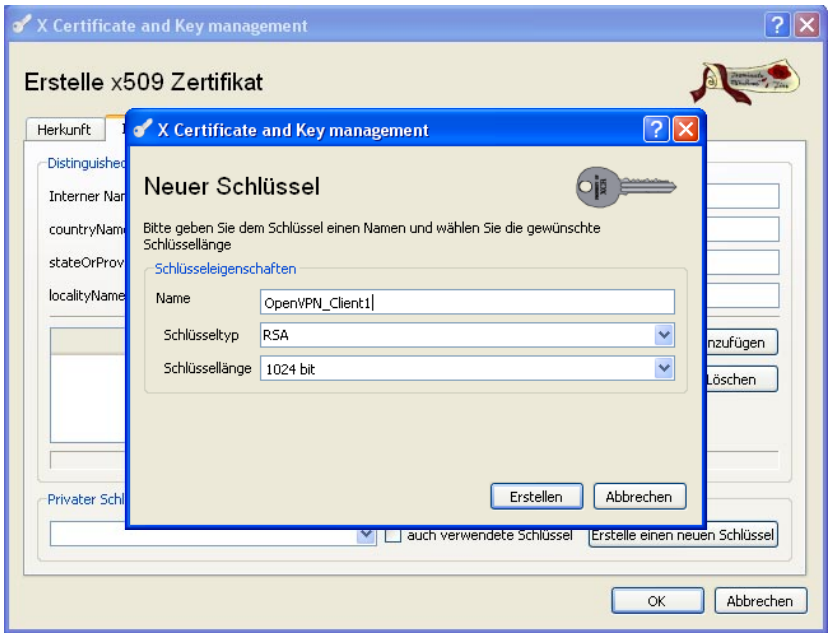


Note:

- *The "commonName" must always be unambiguous!*
- *For example: OpenVPN_Client1, OpenVPN_Client2, etc.*

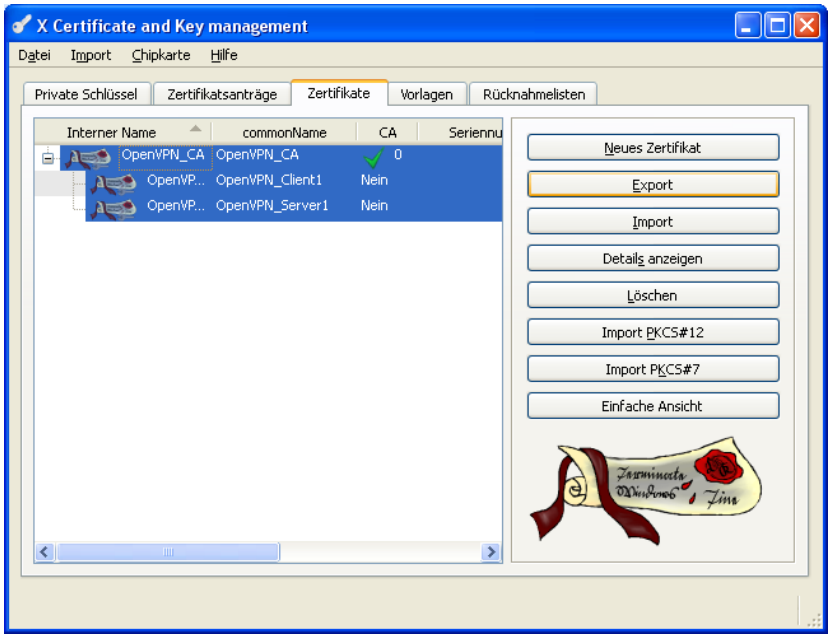


A new key must now be created for every client. (Name = commonName).



EXPORT AS PKCS#12 FILES

For using the paired keys with OpenVPN, the keys can be exported into a PKCS#12 file in a compact form. Go to the "**Certificates**" tab and push the "**Export**" button in order to do this.



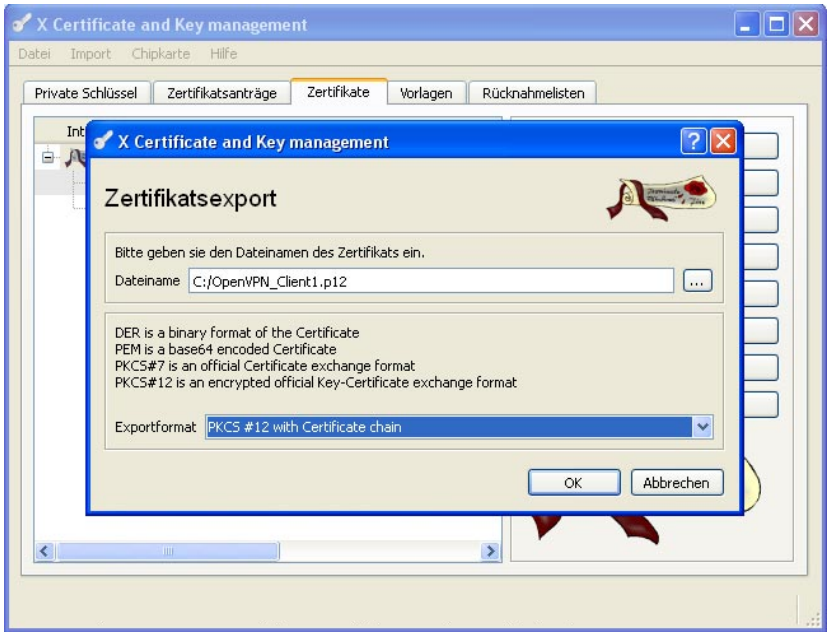
Now highlight (select) all clients and servers you'd like to export, and then push the "**Export**" button.

Then select the desired directory path in which the clients and servers are to be stored in your system.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

Note:

- *Please exclusively select **"PKCS #12 with Certificate Chain**"" as the export format, in order to ensure that the certificate properly works with OpenVPN as well as with the Industrial Firewall.*



Additionally, you can protect the PKCS#12 file with a password. No password should be used for the server, however, since this could prevent the autostart of Linux and Windows XP systems from working. All passwords are needed by the firewall once only - that is during the process of uploading the certificates to the device.

When using VPN clients under Linux or Windows, the password must be entered for every new connection, which is established with the network.

Under certain circumstances, it can be useful to leave all boxes empty and to not assign a password. Protection from unwanted use can also be provided by using a limited validity period instead of a password.

Hint: The server load is reduced, if you set up at the firewall, that the VPN connection is only initiated if the key switch inside the switch cabinet is used.

Select a password which provides high security, if a password is to be used.



INTEGRATING CERTIFICATES IN OPENVPN

If you wish to use certificates on the same PC where the XCA application runs, you'll have to copy these certificates into the OVPN folder, once the certificates have been created and exported.

If you wish to use certificates on your Industrial Firewall, you'll have to ensure that the firewall is connected with a PC and that you have access to the Web interface.

Now, go to "**General / Certificates**" and click on the "**Upload**" button. Look for the folder in which the certificates were stored, and select the one you'd like to upload to the firewall with a double click. If this certificate is protected by a password, you'll have to enter it now.

Go to "**Configuration / OpenVPN**" in order to configure your OpenVPN settings. The uploaded certificate should now be available from the drop down menu.

Please go to the following section for instructions on how to use the p12 file in a regular OpenVPN configuration:

SSL/TLS parms.

See the server config file for more

description. It's best to use

a separate .crt/.key file pair

for each client. A single ca

file can be used for all clients.

Enter the following:

pkcs12 "…OpenVPN\\cert\\OpenVPN_Client1.p12"

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

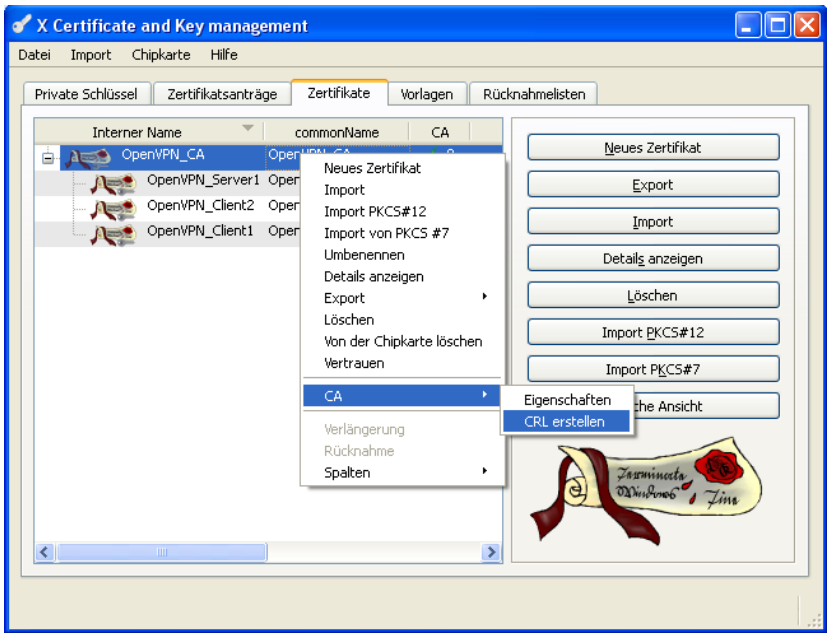
All other file types described in the OVPN file can be ignored.

CREATING A CRL (CERTIFICATE REVOCATION LIST)

XCA additionally offers a function for creating a CRL on the basis of your CA and the chain of certificates.

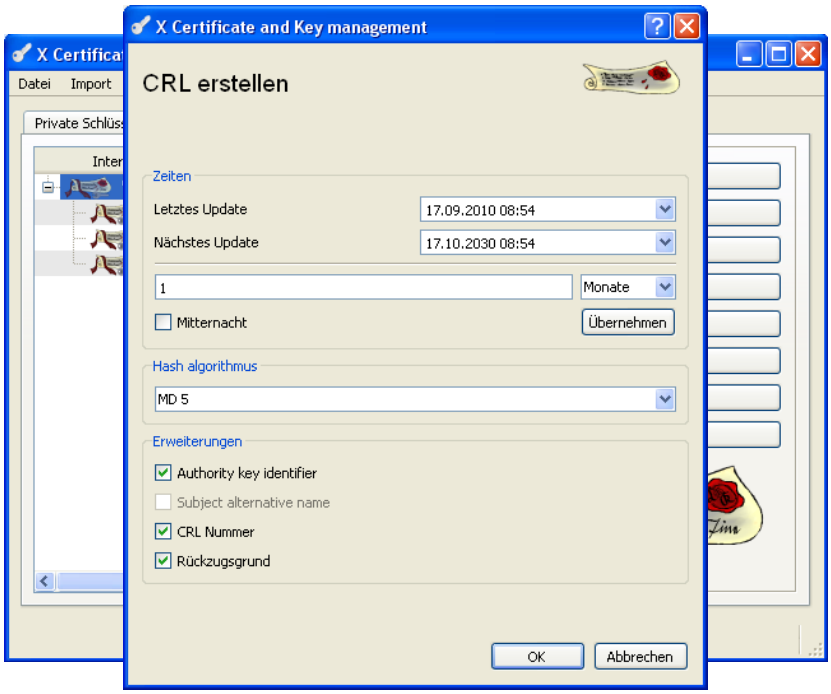
The CRL is a list where all certificates including their respective validity status are included. It allows individual certificates to be withdrawn at the server in a centralised and simplified way.

This is a specific file which is created in XCA and is uploaded to the firewall like a certificate.

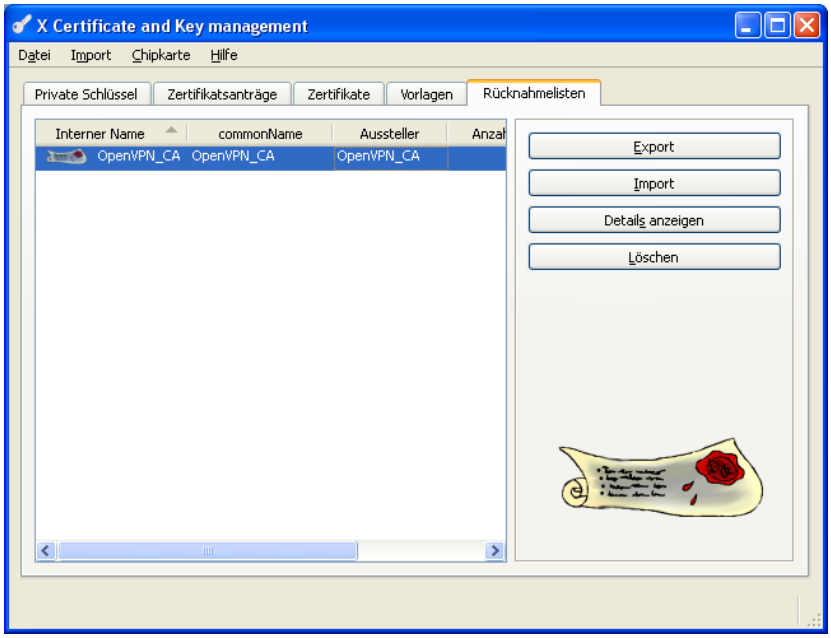


You'll have to determine the validity period as well as the point in time when the next update has to be made. Your next update date should be as far as possible in the future, because usually there is no other reason for creating a new certificate other than the loss of the old certificate.

Tick the three boxes as visualised in the next screenshot and then click on "**OK**".



Once the CRL is created, you can find it in the last tab of the main menu called „**Revocation lists**".



Then click on "**Export**" in order to upload the CRL to the firewall:

Select "PEM" as the file format. The file name assigned by XCA should already be provided with the correct file extension based on the previous selection.

The CRL PEM file is now located in the same folder in which the other certificates have previously been exported. Now proceed as with the upload of regular certificates in order to upload them to the firewall Server:

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

Go to the web interface in **"Configuration / General settings / Certificates"**, click on "Browse" and select the corresponding CRL. Subsequently, you can upload the file to the device by using the "**Upload certificate**" button.

All installed and integrated certificates are verified by using the new CRL. If you wish to renew your trust into a previously revoked certificate, you'll have to select this specific certificate in the XCA programme by clicking on it with the right mouse button, and changing its status to "**Renew certificate**". After that, you'll create a new CRL by exporting and uploading as described above.

If you have a copy of this certificate on your firewall, you will notice that its status in the web interface has also changed to "**Renewed certificate**".

This can be useful in order to temporarily reject VPN access for certain users and machines.

Note:

- *Even if the validity period of a revocation list is expired, it is still used for verification of certificates as long as no newer CRL is available.*
- *The revocation lists of a firewall (a maximum of one list per CA) should always be kept up to date, if possible, in order to avoid creation of security vulnerabilities by lost certificates.*

INCREASED SECURITY WITH DH FILES:

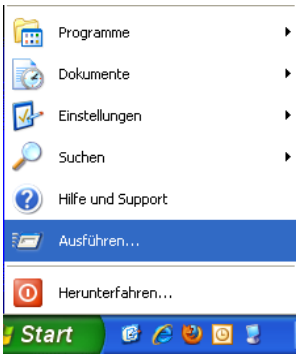
For security reasons, it is recommended to use XCA in connection with an own DH file.

This can be realised by using OpenSSL.

If you don't have OpenSSL yet, you can download it including the default options by using the following link:

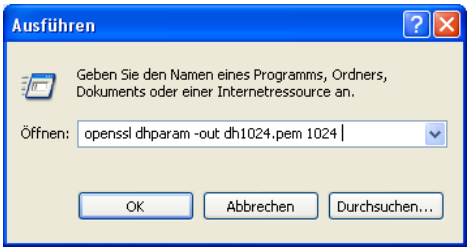
http://www.openssl.org/related/binaries.html

Select "**Start -> Run**" from the start menu after installation. Enter "**CMD**" in the command line and push the "Enter" key.



Then change the directory path to: **C:\OpenSSL-Win32\bin** and enter the following command:

openssl dhparam -out dh1024.pem 1024



The new file dh1024.pem must be saved on the OpenVPN Server, and then provides for an increased security level when used.

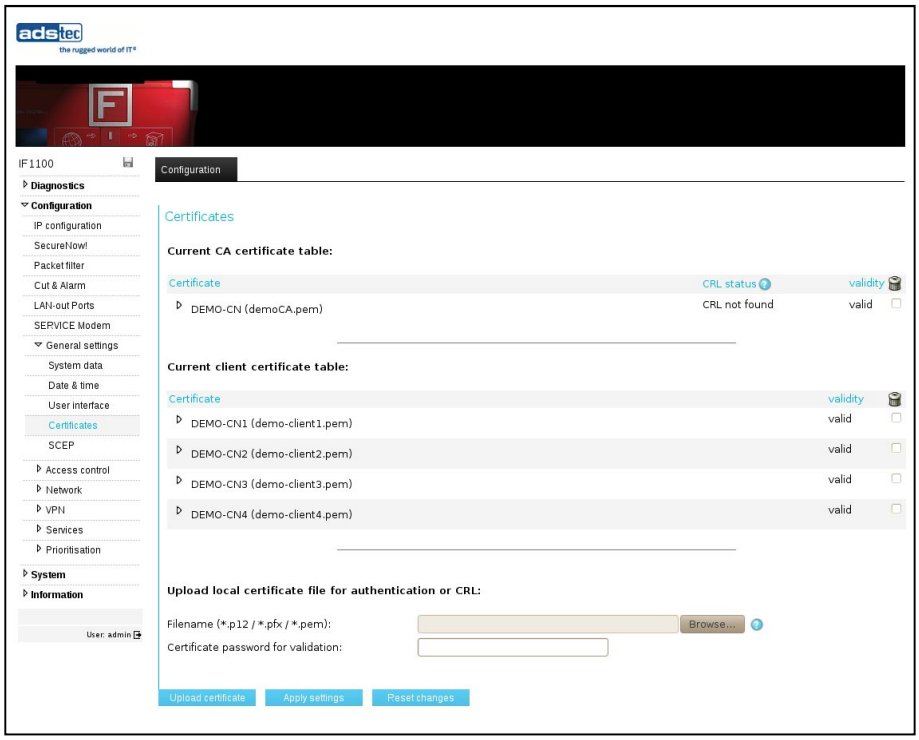
Creating the DH files is going to be integrated in XCA in future as well, but in the current version it still didn't work without any trouble.

ADDITIONAL NOTES

XCA offers many options and additional functions, which could be useful for you in future. Please get in touch with us if you have more questions, or if you require any assistance when creating your certificates.

UPLOADING CERTIFICATES TO THE FIREWALL

CA certificates, regular certificates (client certificates) and revocation lists as well are uploaded to the firewall by using the interface for certificates in the same way. If a valid CA certificate is saved on the firewall, then all certificates which have been signed by this CA are considered as trustworthy, as far as they are not included in a CRL.



© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

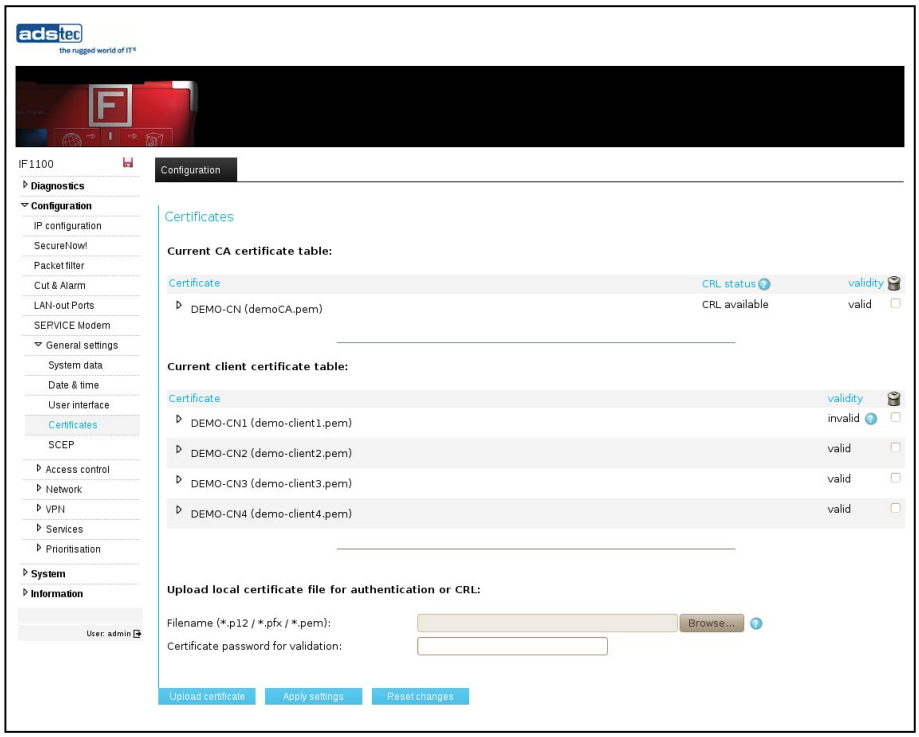
If the PKCS12 container or the certificate itself is provided with a password, this password must be specified when uploading. The actual upload is then carried out using the "Upload certificate" button.

Note:

- *The certificate must either be available as a PKCS12 file or in PEM format including a private key in order to upload it to the firewall.*
- *The private key (e.g. myClient1.key) must be protected from unauthorised access.*
- *With an external CA, the certificate request is generated and submitted to the certification authority. It will verify the specified information and will sign the request (if proper data is provided). The certificate generated in this way may then be used for authentication.*

For deleting a certain certificate, the checkbox next to this certificate below the trash can icon must be unticked and "Apply settings" must be clicked.

If a revocation list exists for a certain CA certificate it will be displayed in the "CRL status" column.



Note:

- *For uploading a certificate as a PEM file, the private key has to be included in the certificate. This does not apply to CA certificates.*
- *A CRL can only successfully be uploaded if the corresponding CA certificate exists in the firewall.*
- *If a CA certificate is deleted, the corresponding CRL file is also automatically deleted.*
- *The demoCA.pem respectively myCA.pem certificates, as well as the demo-*

clientX.pem or myClientX.pem certificates signed with these CA certificates are exclusively used for test purposes, and must never be used for live authentication!

ERROR MESSAGES FOR UPLOADED CERTIFICATES

If a successfully uploaded certificate may actually be used will be indicated in the validity column. If it is invalid, clicking on the small question mark icon will allow you to view the error message in detail.

If the certificate is not yet or no longer valid, the following message will appear:

error 9 at 0 depth lookup: certificate is not yet valid

Solution: The system time must be set correctly. Otherwise, if this is an invalid certificate, a new certificate has to be requested from the issuer.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

If the corresponding CA certificate for a regular certificate is missing, the following message will appear:

error 20 at 0 depth lookup: unable to get local issuer certificate

Solution: The corresponding CA certificate must be uploaded.

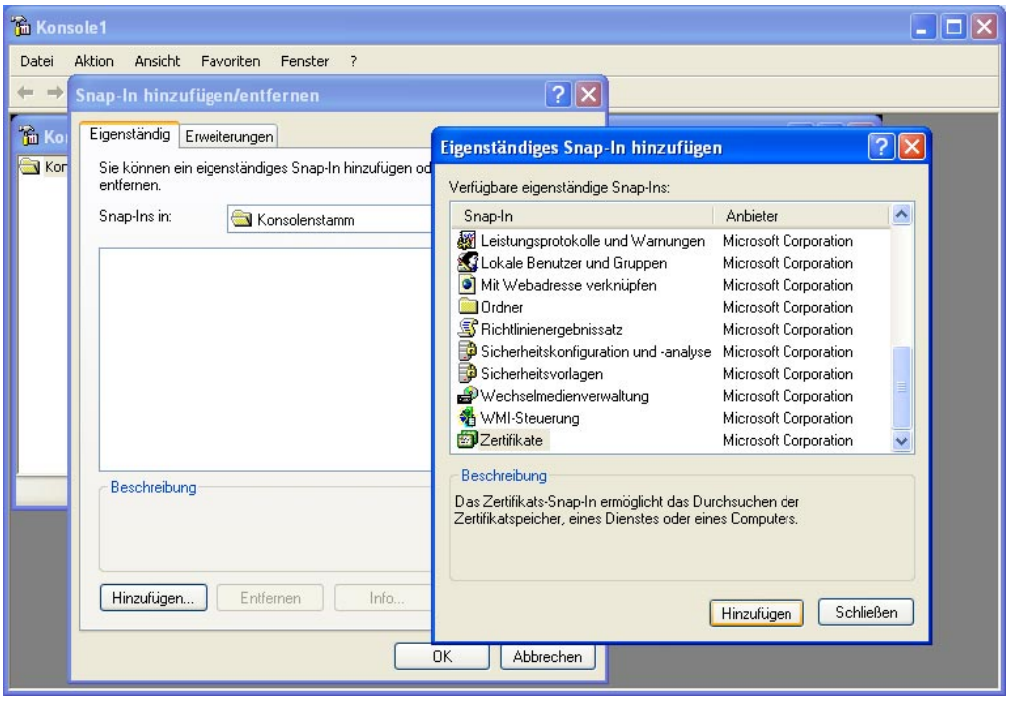
If a regular certificate is uploaded and by mistake exactly the same identity data is used as in the CA certificate with which it was signed, the following message will appear:

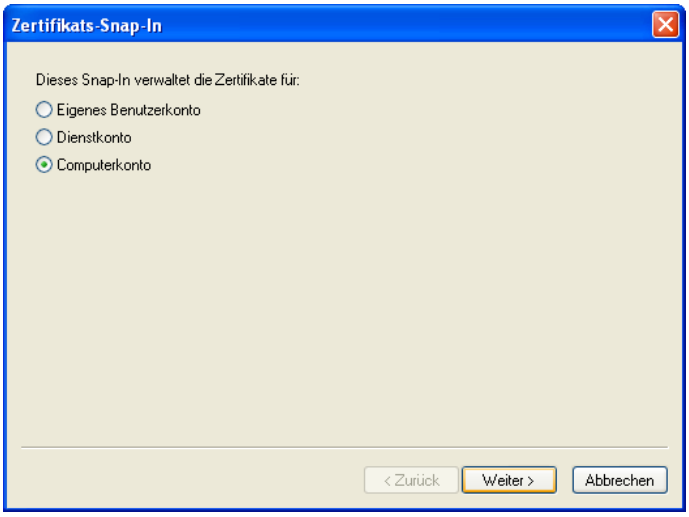
error 7 at 0 depth lookup: certificate signature failure

Solution: The certificate has to be recreated. First, a new client request has to be created where at least one identity field (for instance the Common Name field) must differ from the entries in the CA certificate.

IMPORTING CERTIFICATES UNDER WINDOWS

First the "Microsoft Management Console" programme has to be started. Enter the command mmc in "Start/Run". Within the console, then load the snap-in certificate for the computer account of the local computer by using Add/Remove file/snap-in:

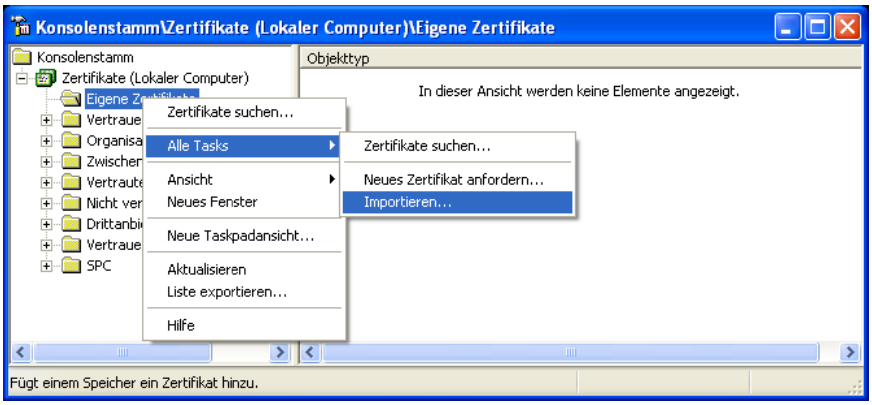




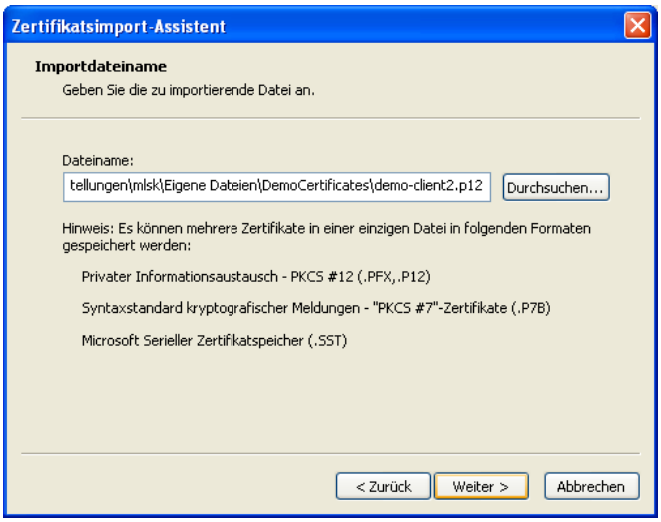
© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen


Computer auswählen
Wählen Sie den Computer aus, den dieses Snap-In verwalten soll.
Dieses Snap-In verwaltet:
Lokalen Computer: (Computer, auf dem diese Konsole ausgeführt wird)
Anderen Computer:
Durchsuchen...
Änderungen zulassen, wenn die Konsole von der Befehlszeile aus gestartet wird. Dies gilt nur, wenn die Konsole zuvor gespeichert wurde.
< Zurück
Fertig stellen
Abbrechen

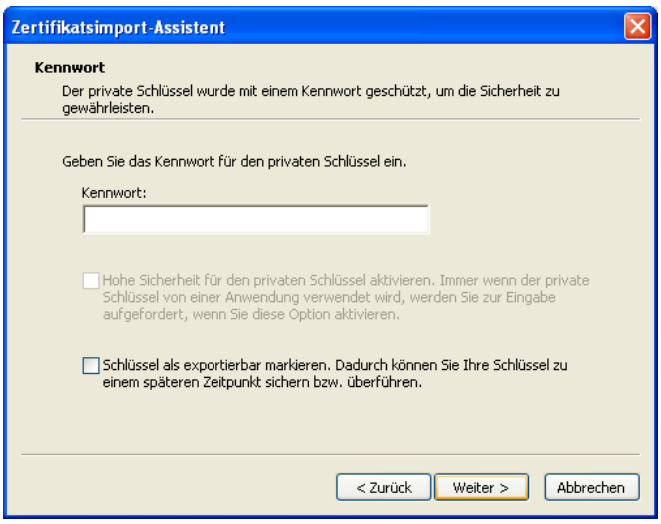
The menu is opened by right-clicking on the certificate folder. The certificate wizard is then started by using the All tasks/Import option:



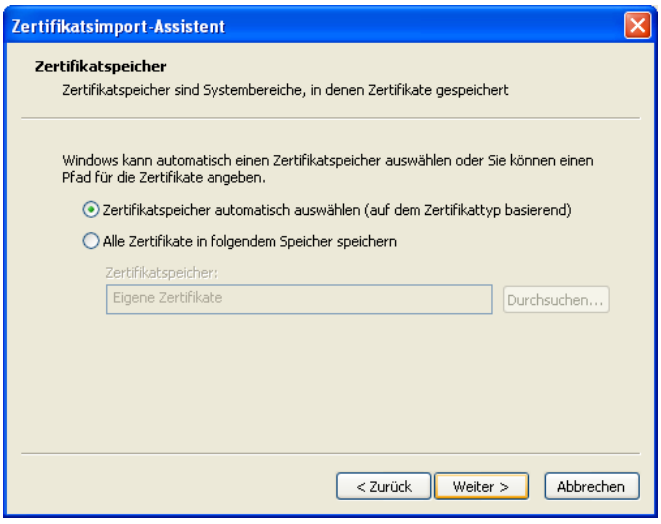
Next the certificate file has to be selected:


Zertifikatsimport-Assistent
Importdateiname
Geben Sie die zu importierende Datei an.
Dateiname:
tellungen\mlsk\Eigene Dateien\DemoCertificates\demo-client2.p12
Durchsuchen...
Hinweis: Es können mehrere Zertifikate in einer einzigen Datei in folgenden Formaten gespeichert werden:
Privater Informationsaustausch - PKCS #12 (.PFX,.P12)
Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B)
Microsoft Serieller Zertifikatspeicher (.SST)
< Zurück
Weiter >
Abbrechen

If the container or the certificate is password protected, this password must be specified for importing (for the exemplary demo-client2.p12 container, there is no password, which is why you may press the Next button directly):

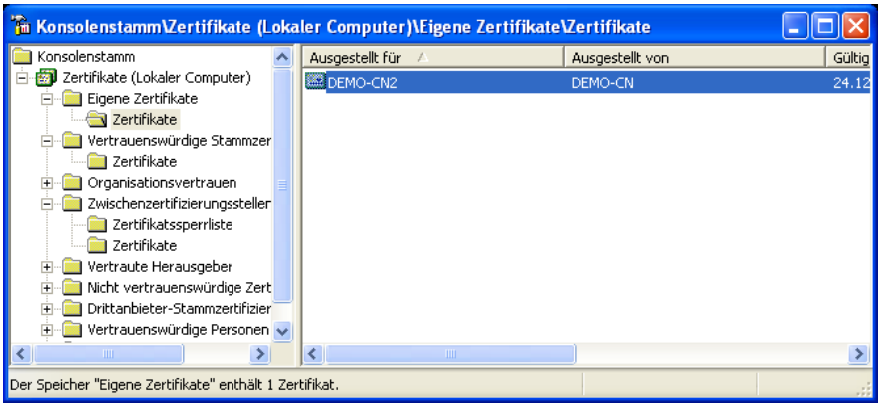

Zertifikatsimport-Assistent
Kennwort
Der private Schlüssel wurde mit einem Kennwort geschützt, um die Sicherheit zu gewährleisten.
Geben Sie das Kennwort für den privaten Schlüssel ein.
Kennwort:
Hohe Sicherheit für den privaten Schlüssel aktivieren. Immer wenn der private Schlüssel von einer Anwendung verwendet wird, werden Sie zur Eingabe aufgefordert, wenn Sie diese Option aktivieren.
Schlüssel als exportierbar markieren. Dadurch können Sie Ihre Schlüssel zu einem späteren Zeitpunkt sichern bzw. überführen.
< Zurück
Weiter >
Abbrechen

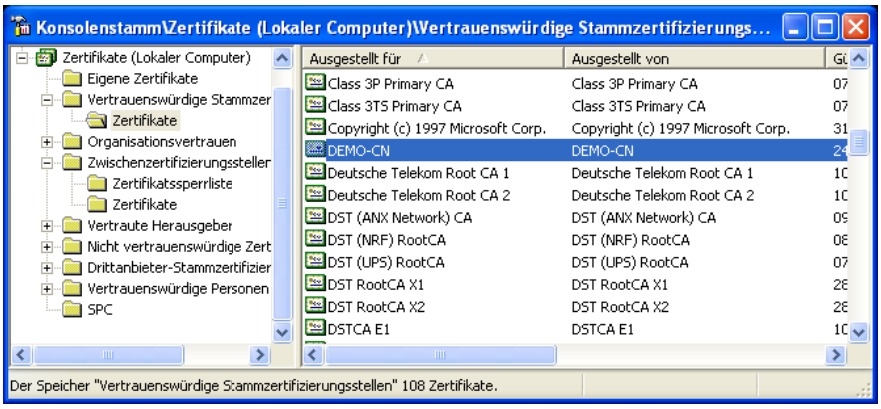
Certificates must be sorted automatically (so that e.g. demo-client2.pem as a certificate and demoCA.pem as a root certificate is sorted out of the demo-client2.p12 PKCS12 container):


Zertifikatsimport-Assistent
Zertifikatspeicher
Zertifikatspeicher sind Systembereiche, in denen Zertifikate gespeichert
Windows kann automatisch einen Zertifikatspeicher auswählen oder Sie können einen Pfad für die Zertifikate angeben.
Zertifikatspeicher automatisch auswählen (auf dem Zertifikattyp basierend)
Alle Zertifikate in folgendem Speicher speichern
Zertifikatspeicher:
Eigene Zertifikate
Durchsuchen...
< Zurück
Weiter >
Abbrechen

Finally, import must be completed. Certificates may then be viewed under My certificates, and root certificates under Trusted root certificates. These folders might have to be updated first (right-click and select the Update item in the menu).

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen





Note:

- *The PKCS12 file contains also the demoCA.pem root certificate, apart from the actual demo-client2.pem certificate.*
- *If the root certificate is not included in the container in case of My certificates (own certificates), it must be imported in the same way.*

11.10 SCEP

GENERAL

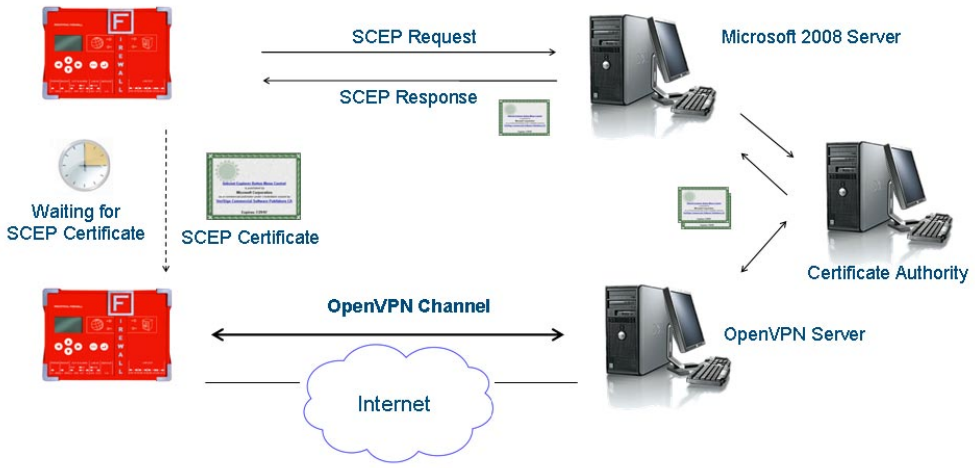
The "Simple Certificate Enrolment Protocol" was developed with the intent of making the distribution of certificates as simple and scalable as possible. The current status (as per 30th November 2009) is defined in the IETF draft, which you'll find at http://tools.ietf.org/id/draft-nourse-scep-20.txt .

Precisely one certificate can be uploaded into the ads-tec device by using SCEP. This certificate is then available for all certificate based services, just like a manually created and uploaded certificate. The benefit of SCEP is, that all devices of a certain type can be set up with the same configuration in one go, as long as we consider an environment with several ads-tec infrastructure products (e.g. by using IDA), and can then individually obtain the certificates they require.

The prerequisite is that a PKI (public key infrastructure) including a registration authority (RA) exists, which supports the Simple Certificate Enrolment Protocol. This is possible with a Windows Server CA (certificate authority), with which the NDES service (network device enrolment service) is installed (also possible as an individual RA server) or with a Linux Server in connection with OpenSSL and OpenSCEP.

Note:

Since the validity of certificates is always restricted to a certain period of time, all devices must have the correct system time setting. We urgently recommend using the NTP (network time protocol) service on all devices in order to ensure the correct time on all devices at all times.



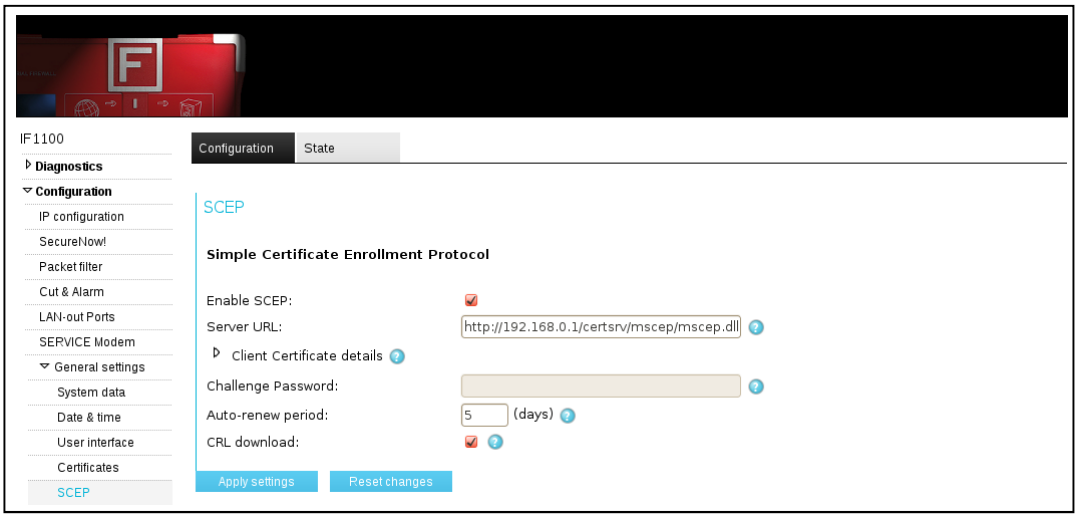
The figure shows the procedure of a certificate request by using SCEP. Once the required SCET data is set up on the firewall (e.g. the SCEP server URL), the certificate request is generated, which is submitted to the SCEP server. The CA and SCEP certificates are retrieved from the SCEP server beforehand (not shown in the figure). In this way the subsequent communication is protected from any manipulation.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

Then the SCEP server forwards the request to the CA. The firewall retrieves the process status ("Waiting for SCEP certificate" status in this figure) in regular intervals until the SCEP server has obtained the desired certificate from the CA.

Once the certificate is approved and issued by the CA, it is downloaded from the IFW via the SCEP server. If OpenVPN connections, which use the SCEP certificate (and which is not yet available) are already configured at this point in time, then these connections are automatically started now.

CONFIGURATION



All basic settings with respect to the SCEP server and the certificates are made on the SCEP main page. The setting "Enable SCEP" must be selected in order to enable SCEP. More settings can be made after that.

The SCEP "Server URL" setting is of utmost importance. To be valid, the entry has to be made in the form http://SCEP_SERVER/PATH, where "SCEP_SERVER" can be either an IP address or a DNS name in this case. The PATH depends on the SCEP server software. If for instance the NDES Windows Server is used, then "certsrv/mscep/mscep.dll" is usually the correct path.

In order to allow the SCEP service to verify the SCEP server / RA, it is required that the CA certificate, with which the SCEP server certificate has been signed, is uploaded to the firewall beforehand. The SCEP server certificate and the CA certificate are then automatically obtained, verified and subsequently displayed on the "Certificates" page.

EXAMPLE:

The PKCS12 file contains also the demoCA.pem root certificate, apart from the actual demo-client2.pem certificate.

If the root certificate is not included in the container in case of My certificates (own certificates), it must be imported in the same way.

Challenge password:

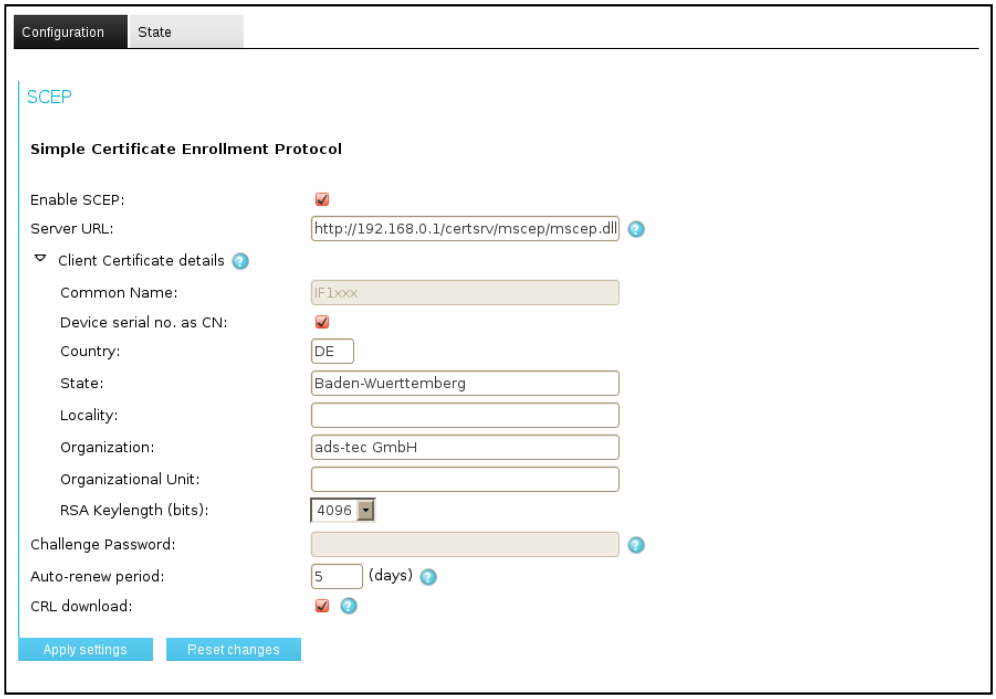
The challenge password is a "disposable password" in most cases, i.e. it can only be used exactly once. This prevents under certain circumstances that unauthorised people can obtain a certificate from the CA and has therefore a vital role in particular with publically available CAs.

Renewal interval:

If a challenge password is not set, a number of days can be defined here. It tells you how many days before the certificate expiry date a new certificate is automatically obtained via SCEP.

Automatic CRL download: This option is used for the automatic retrieval of an up-to-date CRL from the CA. Once started, it tries to obtain an updated CRL every hour. If a new CRL was successfully obtained, it is displayed on the "Certificates" page including the related CA certificate.

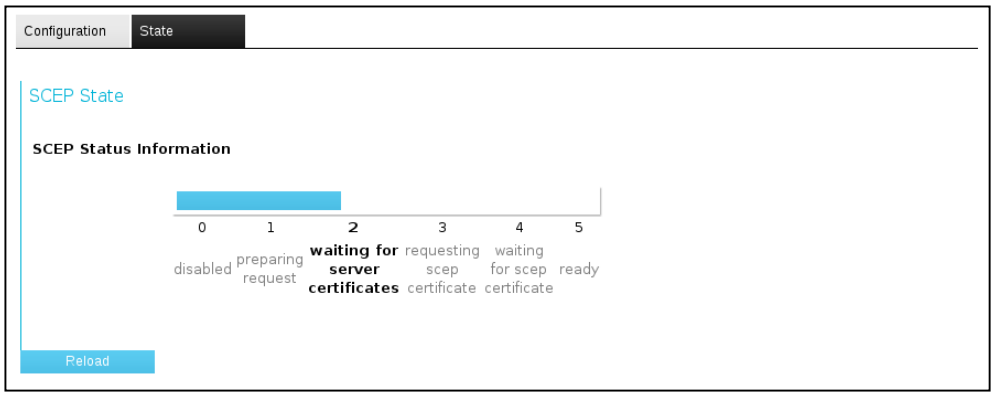
CLIENT CERTIFICATE DETAILS:



More setup options concerning the properties of the certificate appear if you click on the "Client certificate details" button. Frequently used "Distinguished name" boxes and the length of the RSA key belonging to the certificate can be defined here.
With the "Use device serial number as name" option, the combination "Device_type-serial_number (e.g. IF1100-AX00900071) is used as the "Common name". This option is important if several devices with the same configuration are set up. Since the serial number is different for every individual device, this ensures that every device is provided with a certificate with individual properties.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

STATUS PAGE

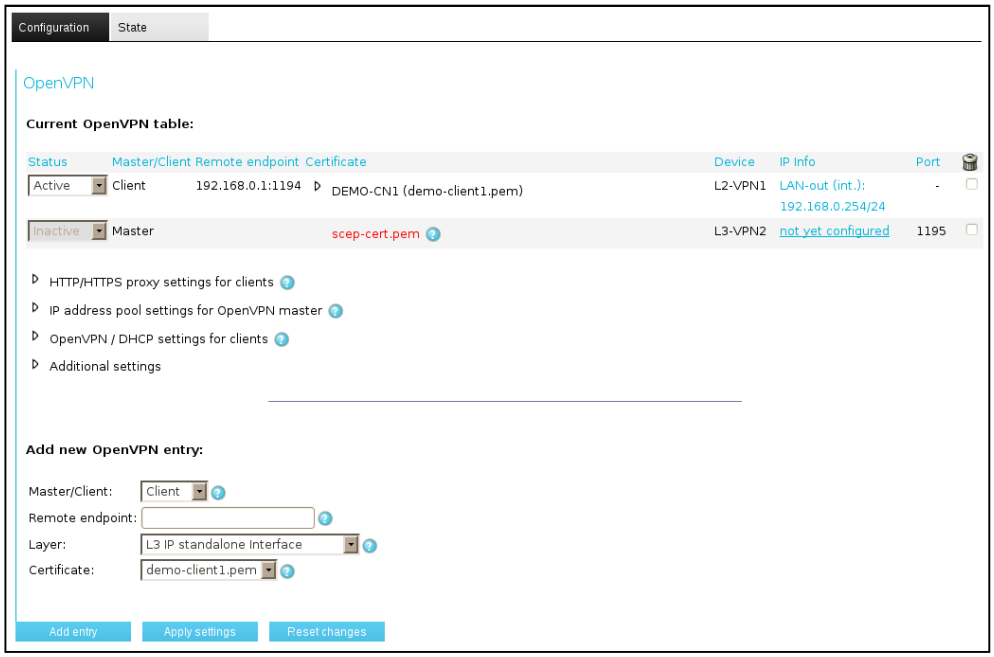


You can reach the status page from the SCEP main page by using the "Status" tab. The progress bar in this tab displays the current status.
If the bar has reached the "5 - completed" position, the certificate is available on the "Certificate" page and can be used like all the other certificates.
In the event of an error, detailed error messages, which provide notes regarding the error cause, appear underneath the progress bar.

USE OF OPENVPN WITH A CERTIFICATE

It is possible to use the "scep-cert.pem" certificate with OpenVPN connections, although the SCEP service is probably not enabled at all, or the SCEP request is not completed yet. These connections are only enabled once the certificate has successfully been obtained via SCEP.

As long as the "scep-cert.pem" certificate is not available yet, the certificate is displayed with a red font colour on the OpenVPN page. After the successful download, the font colour is switched to black, and more certificate details can be displayed.





Note:

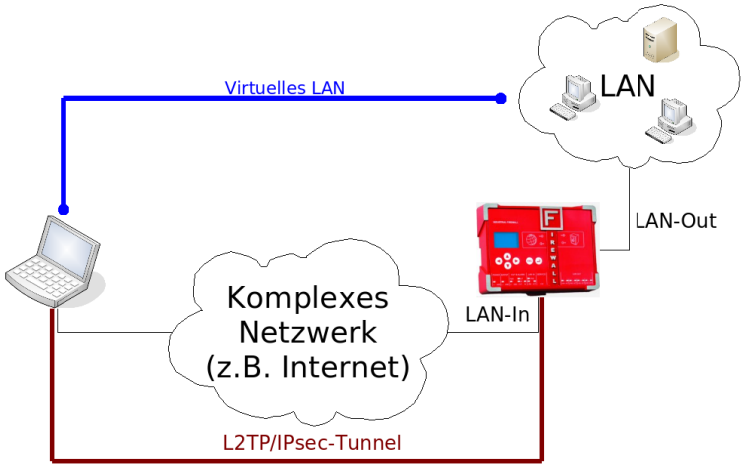
Windows Server NDES is using the "IPSEC Intermediate (offline)" certificate template as a default setting. This template cannot be used for OpenVPN connections, since it is not intended for client and server authentication in accordance with the "x509 v3 extended key usage". With Windows Server 2003, there is additionally no other opportunity of using a different template for NDES. If Windows Server 2008 is used, a different template can be set up via the registry (directory path: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP).

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

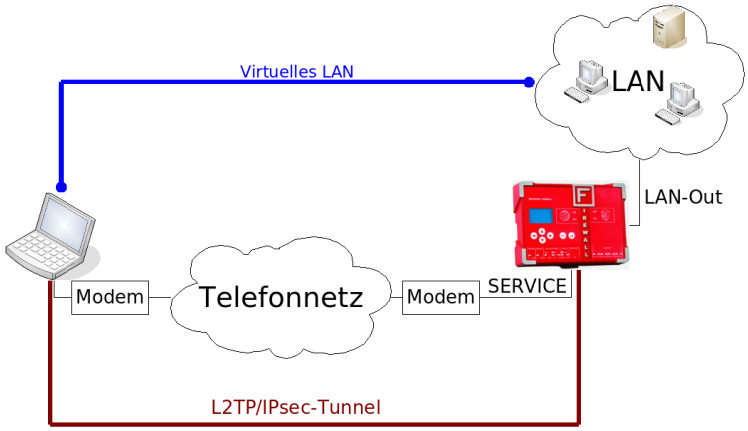
11.11 L2TP

GENERAL

The "Layer 2 Tunnelling Protocol" (L2TP) is a tunnelling solution for setting up a virtual private network (VPN). IPsec is used for encrypting the connection. The IF1100 may be used as a L2TP/IPsec server and thus allow the secure connection of external clients. For instance via DSL by using LAN-in:



Or via modem using SERVICE:



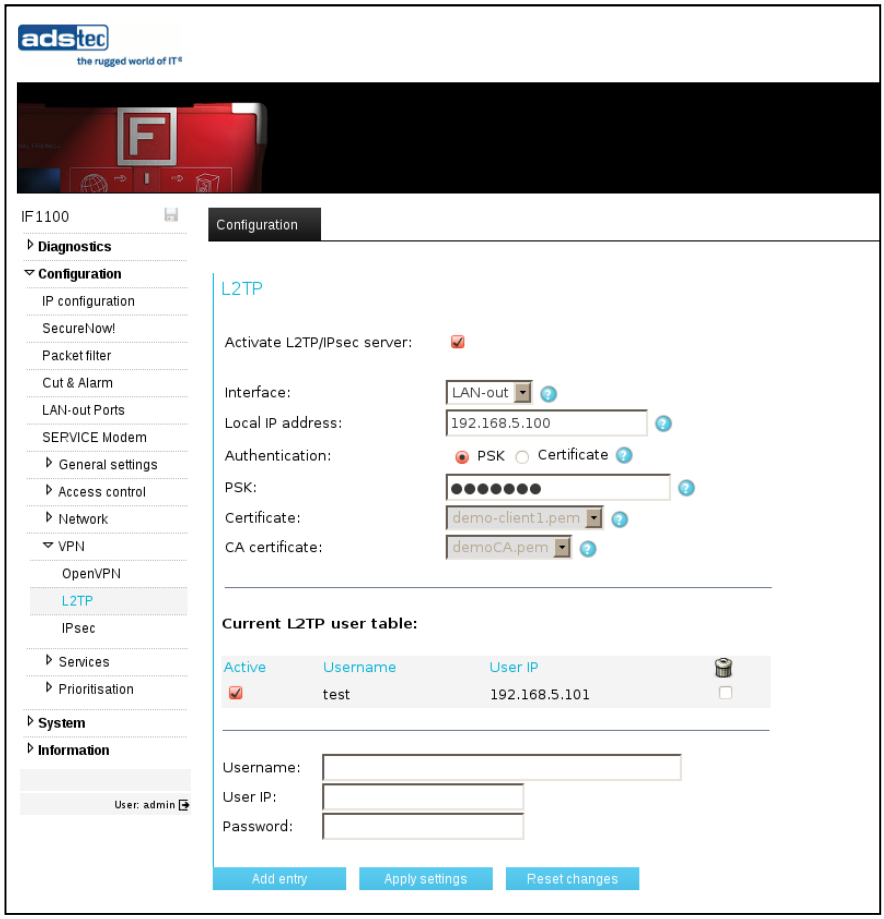
In our exemplary configuration for LAN-in, the server is using the IP addresses 191.168.11.164 (LAN-in) and 192.168.5.164 (LAN-out). The gateway is using the IP addresses 192.168.11.166 (LAN-in) and 192.168.1.166 (LAN-out). The client with the IP address 192.168.1.168 is connected with the NAT gateway via LAN-out (the server thus does not see the client IP-address but only the gateway IP-address). The L2TP connection is configured in such way, that the client endpoint gets the IP address 192.168.5.101, and thus becomes a subscriber of the LAN-out network of the server by using the VPN tunnel.



Note:

IPsec and L2TP/IPsec are exclusive services and may not run at the same time. As soon as the L2TP/IPsec service is activated, the pure IPsec service is disabled and vice versa.

FIREWALL CONFIGURATION AS L2TP/IPSEC SERVER FOR LAN-IN WITH PSK



The interface of the local tunnelling endpoint, its local IP address and the type of authentication can be specified in the upper section of the configuration page for L2TP/IPsec. Users are added in the lower half (user name, password and IP address). In our example, the server is using IP address 192.168.5.100, and assigns the IP address 192.168.5.101 to the client. These addresses are included in the LAN-out subnet (192.168.5.0/24). As a result, the client becomes a component of the LAN-out network via the secure L2TP/IPsec connection.

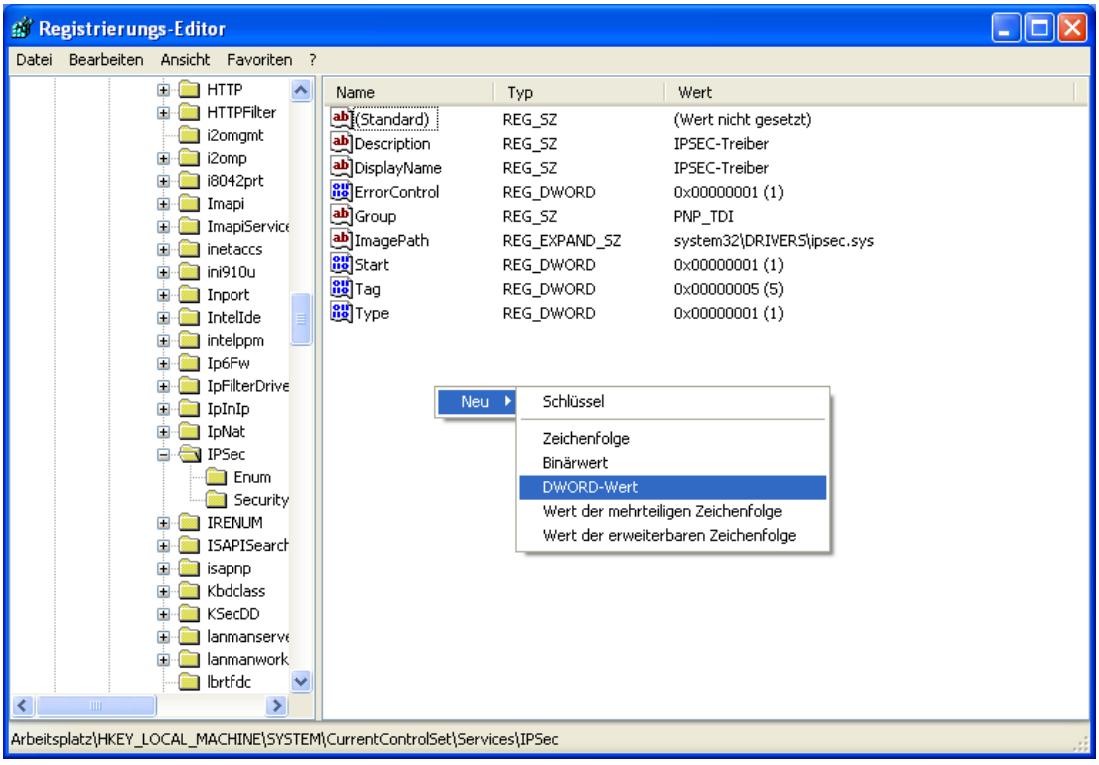
Note:

The local IP address and the user IP addresses must not have been assigned yet. User name and password are used by the client in order to login at the server (see next passage)

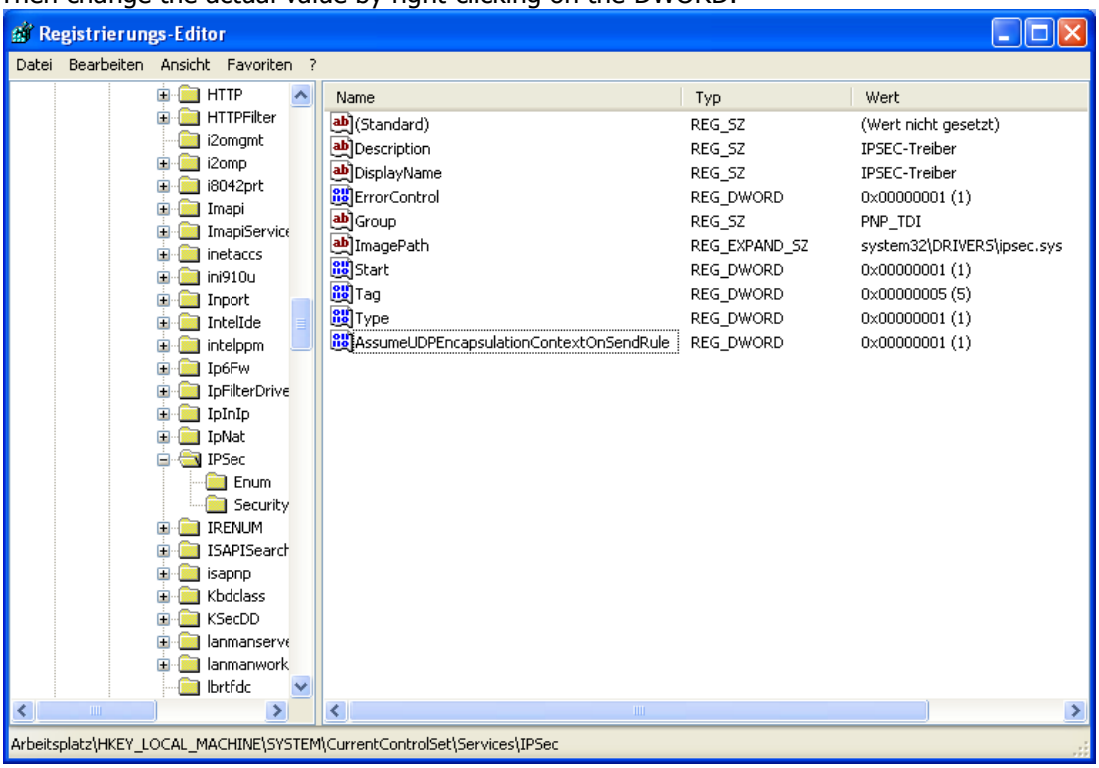
© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

CONFIGURATION OF WINDOWS XP AS AN L2TP/IPSEC CLIENT WITH PSK

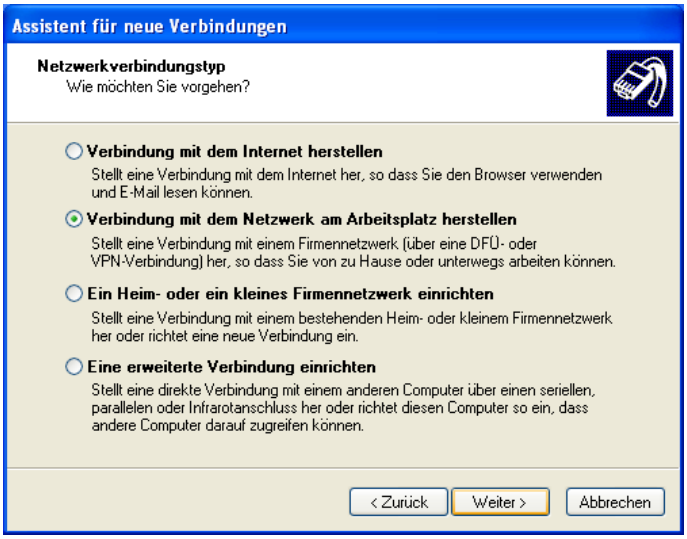
First an entry must be added in the Windows registry. The registry editor can be started with the "regedit" command in the "Start/Run..." command line. The DWORD AssumeUDPEncapsulationContextOnSendRule under HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/IPSEC must be set to 1. Create the DWORD by right-clicking and using New/Create DWORD value first.



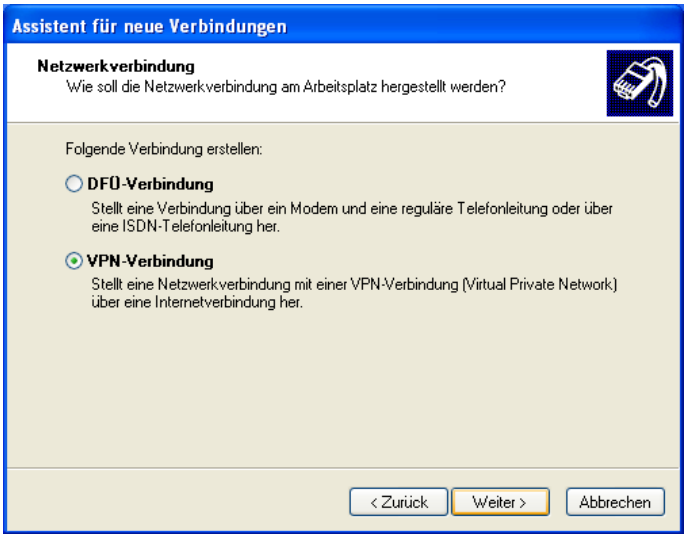
Then change the actual value by right-clicking on the DWORD.



Open the Network connections view via Control Panel/Network connections and start the wizard there by using View network connections/Create a new connection. Select Connect to the Network at my Workplace for the network connection type:

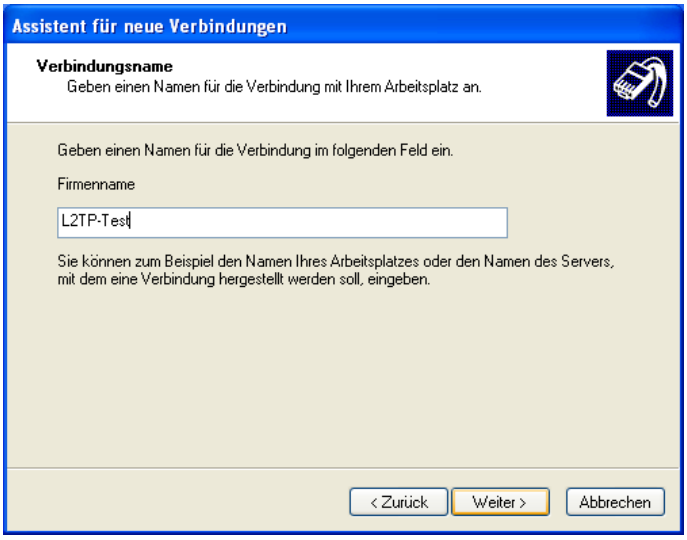

Assistent für neue Verbindungen
Netzwerkverbindungstyp
Wie möchten Sie vorgehen?
Verbindung mit dem Internet herstellen
Stellt eine Verbindung mit dem Internet her, so dass Sie den Browser verwenden und E-Mail lesen können.
Verbindung mit dem Netzwerk am Arbeitsplatz herstellen
Stellt eine Verbindung mit einem Firmennetzwerk (über eine DFÜ- oder VPN-Verbindung) her, so dass Sie von zu Hause oder unterwegs arbeiten können.
Ein Heim- oder ein kleines Firmennetzwerk einrichten
Stellt eine Verbindung mit einem bestehenden Heim- oder kleinem Firmennetzwerk her oder richtet eine neue Verbindung ein.
Eine erweiterte Verbindung einrichten
Stellt eine direkte Verbindung mit einem anderen Computer über einen seriellen, parallelen oder Infrarotanschluss her oder richtet diesen Computer so ein, dass andere Computer darauf zugreifen können.
< Zurück
Weiter >
Abbrechen

Select Virtual Private Network connection for the connection type:

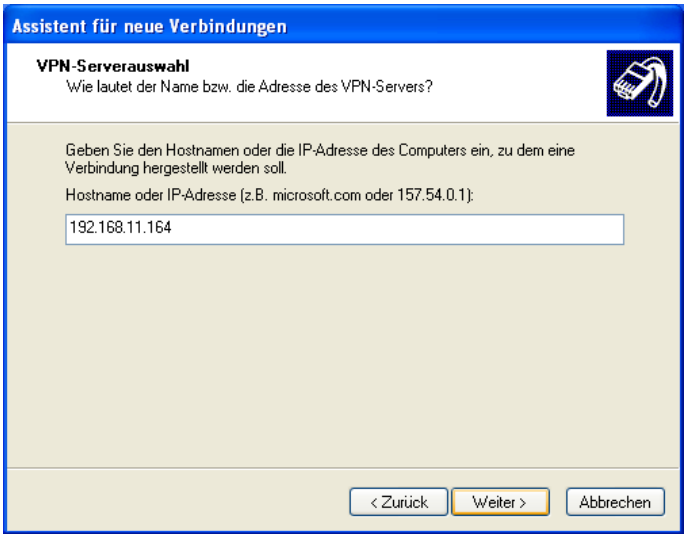

Assistent für neue Verbindungen
Netzwerkverbindung
Wie soll die Netzwerkverbindung am Arbeitsplatz hergestellt werden?
Folgende Verbindung erstellen:
DFÜ-Verbindung
Stellt eine Verbindung über ein Modem und eine reguläre Telefonleitung oder über eine ISDN-Telefonleitung her.
VPN-Verbindung
Stellt eine Netzwerkverbindung mit einer VPN-Verbindung (Virtual Private Network) über eine Internetverbindung her.
< Zurück
Weiter >
Abbrechen

As the Connection Name you can use L2TP test, for example:

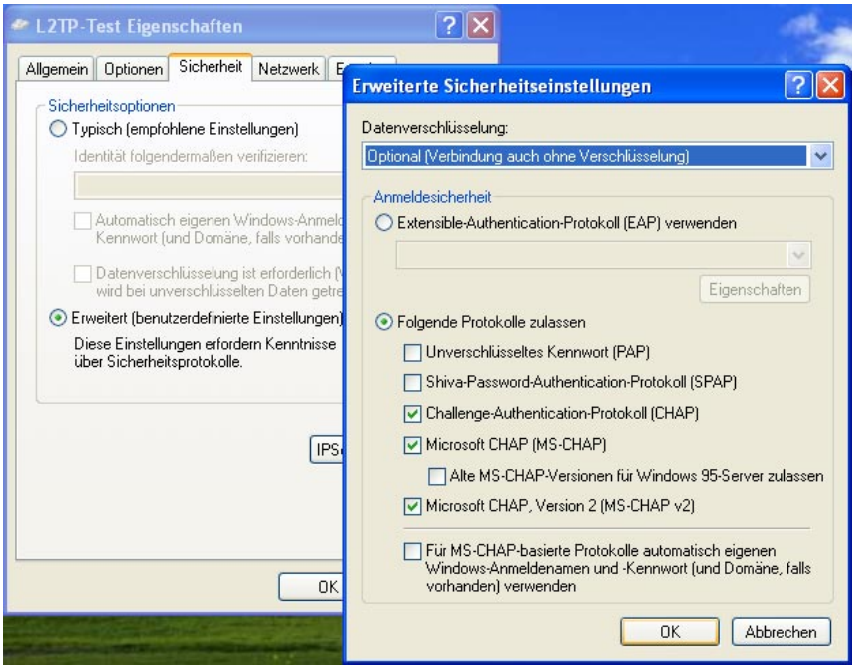
© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen


Assistent für neue Verbindungen
Verbindungsname
Geben einen Namen für die Verbindung mit Ihrem Arbeitsplatz an.
Geben einen Namen für die Verbindung im folgenden Feld ein.
Firmenname
L2TP-Test
Sie können zum Beispiel den Namen Ihres Arbeitsplatzes oder den Namen des Servers, mit dem eine Verbindung hergestellt werden soll, eingeben.
< Zurück
Weiter >
Abbrechen

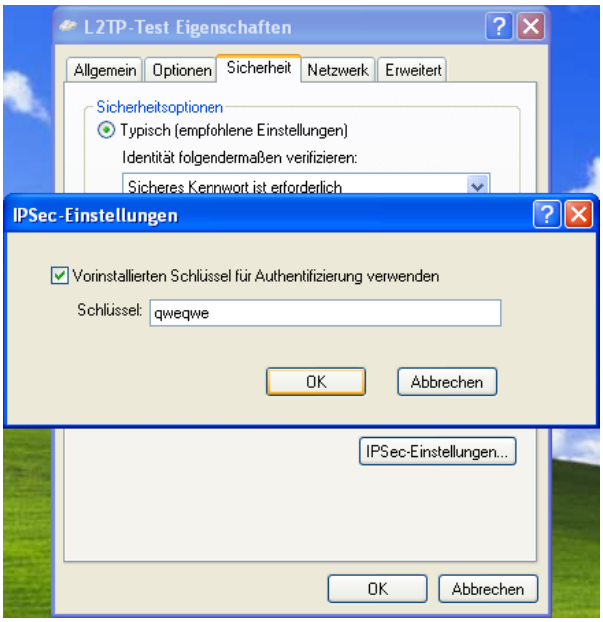
The server IP address is 192.168.11.164, for instance:


Assistent für neue Verbindungen
VPN-Serverauswahl
Wie lautet der Name bzw. die Adresse des VPN-Servers?
Geben Sie den Hostnamen oder die IP-Adresse des Computers ein, zu dem eine Verbindung hergestellt werden soll.
Hostname oder IP-Adresse (z.B. microsoft.com oder 157.54.0.1):
192.168.11.164
< Zurück
Weiter >
Abbrechen

Finally, the connection setup is completed. Before you can now establish the VPN with a right-click on the new icon and by using Connect, some settings have to be adapted (in the Connect dialogue). First you must select Advanced under Properties > Security options and set the Data encryption there to Optional encryption:

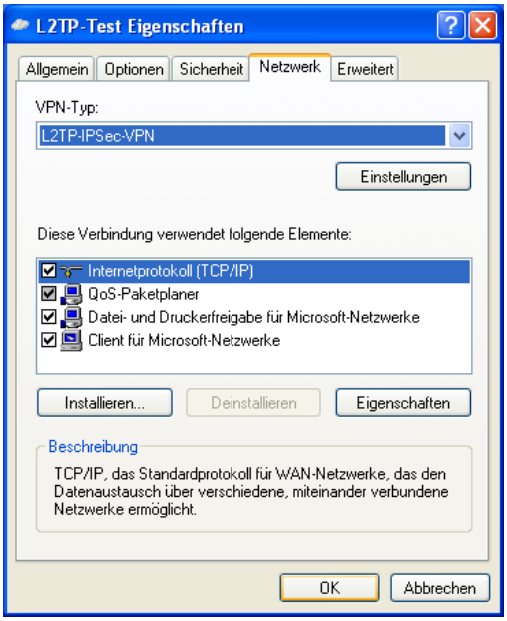


The PSK must be specified under Security/IPsec settings (qweqwe in the example):



The VPN type must be set to L2TP-IPsec-VPN under Networking:

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen



Now the connection can be established by using a User name and a Password (test in the example in both cases):



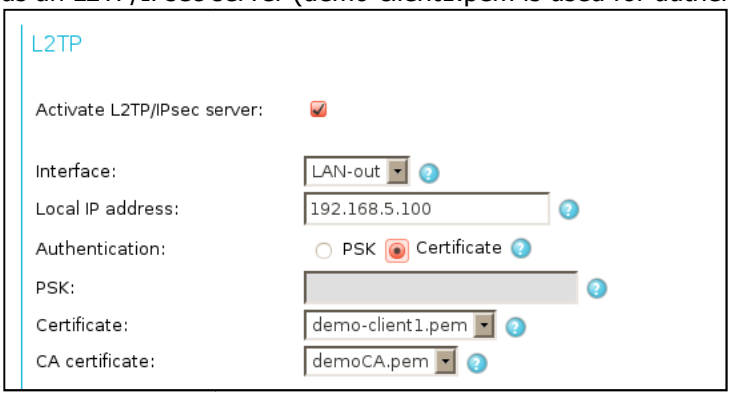
Note:

The L2TP function was only tested with Windows XP professional. Other operating systems should also work. However, certain updates might be required or limitations might exist. For example, PSK cannot be used under Windows 2000. Authentication must be carried out using certificates in that case (see next passage).

If the client is not located behind the router (but directly connected with the Internet), and if you experience problems when establishing the connection, the AssumeUDPEncapsulationContextOnSendRule Windows-registry value should be set to 0.

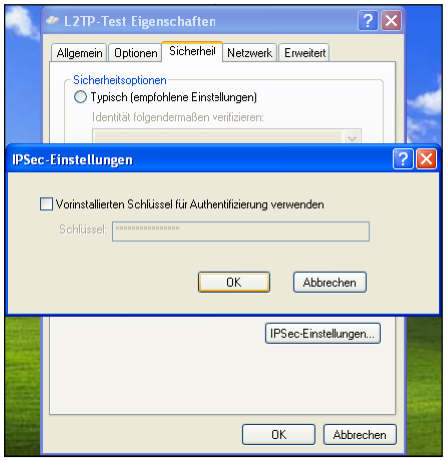
CONFIGURATION OF WINDOWS XP PROFESSIONAL AS AN L2TP CLIENT WITH CERTIFICATES

A change in Authentication (method) to Certificates is required at the firewall which works as an L2TP/IPsec server (demo-client1.pem is used for authentication in the example):



Under Windows, a certificate must be uploaded into the certificate memory (for example demo-client2.p12). Additionally, a root certificate is required for authentication of the remote terminal (e.g. demoCA.pem; it is included in the PKCS12 container, already).

Defining the VPN network connection is carried out as described in the previous section, but with the difference that no pre-installed key (and thus automatically a certificate) is used:





Note:

How to create certificates, upload them to the firewall and import them under Windows is described in the "Certificates" use case.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

CONFIGURATION OF WINDOWS XP PROFESSIONAL AS AN L2TP CLIENT WITH CERTIFICATES USING A MODEM

This feature is currently unavailable due to an interoperability issue caused by Windows. A laptop, for instance, is currently unable to dial in at the firewall and to additionally start an L2TP connection.

Should, however, the network connection be established between a Dial-out and a Dial-in firewall via modem (refer to our "SERVICE" use case), and the L2TP connection be established to the second firewall, configuration is carried out in the same way as described for the example of L2TP/IPsec tunnelling via LAN-in. Connecting a laptop to a firewall via SERVICE and establishing a tunnel to the firewall behind it, also works in the same way.



Note:

If in a firewall SERVICE and L2TP are activated for the SERVICE interface, the user name of the SERVICE interface must differ from the L2TP user name.

11.12 IPsec

General

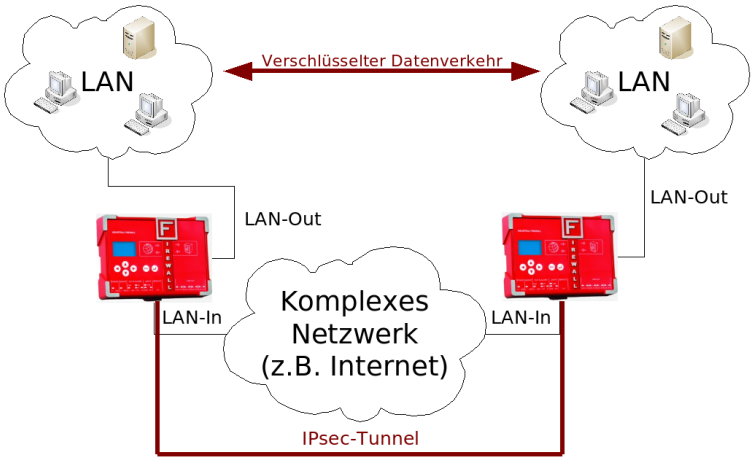
IPsec allows the encoding of the entire communication with a remote endpoint on an IP level. Establishment is carried out in two steps. First, both parties authenticate each other (Main mode), and then the actual tunnel is established (Quick mode). Authentication is either carried out by using certificates (recommended) or by using a Pre-Shared Key (or short PSK, which is less safe than a certificate).

Note:

Please refer to the "Certificates" use case for creating and uploading of certificates.

"Subnet-to-subnet" use case

In this use case, an IPsec tunnel is established between two firewalls and the entire data traffic between two dedicated subnets is encrypted. Up to 64 connections may be defined on the IF1000 firewall. The local subnet is the same for all connections, in this case.



Note:

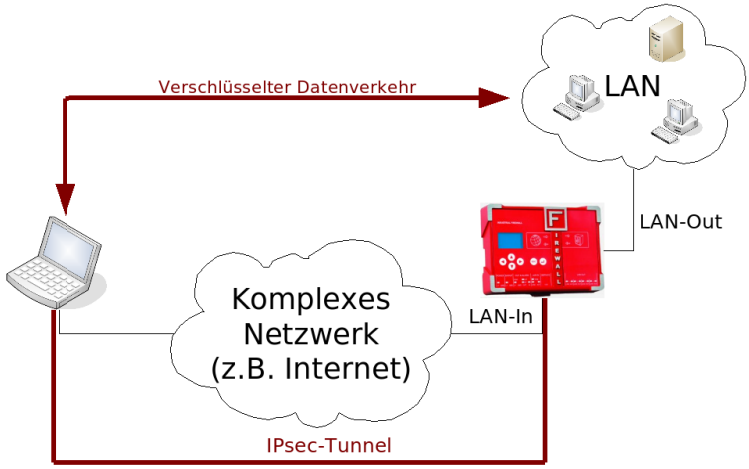
IPsec encrypts the data traffic between two dedicated subnets, only. In order to encrypt the entire data traffic between two firewalls, the 0.0.0.0/0 subnet, which includes all possible subnets, must specifically be used.

The subnets of both remote terminals must differ from the local subnet, so that the data traffic can properly be allocated.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

"ROADWARRIOR" USE CASE

In this case, a so-called "roadwarrior" (e.g. a "moving" laptop from a hotel room) establishes an IPsec connection with a firewall and gains access to a network behind the firewall (e.g. to an entire company network) in an encrypted way.



Note:

*Any number of roadwarriors is allowed to connect with the firewall by using the roadwarrior connection type. However, only the data traffic of the roadwarrior itself (but not the traffic of a potential subnet behind it) is encrypted in each case. Only one roadwarrior connection can exist on the firewall (remote IP address and remote subnet are both set to *).*

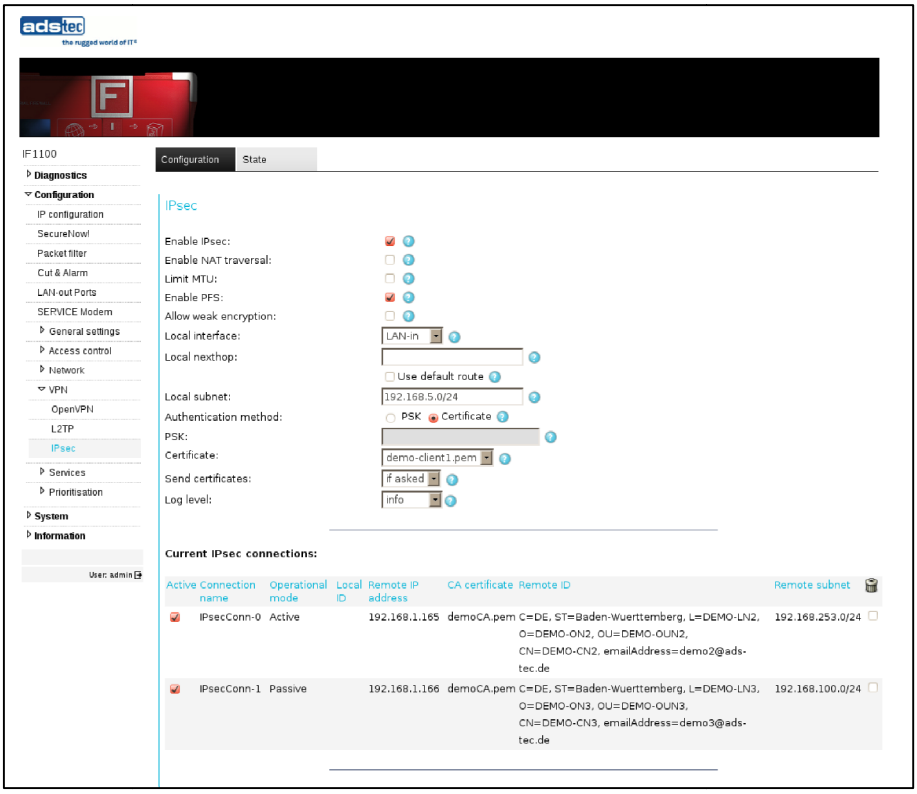
"SUBNET-TO-SUBNET" CONFIGURATION

Both endpoints of an IPsec tunnel are equivalent peers. This shows that it is not about a server/client model. Therefore, the configuration of both parties is generally the same, with the difference that the definition of subnet and remote endpoint must be inverted accordingly.

In this example, the "West" and "Southwest" firewalls are supposed to establish a tunnel with the "East" firewall. All three devices are connected with a switch on the LAN-In interface (192.168.1.0/24 network). The data traffic between the LAN-out networks is to be encrypted. "West" has the end number 165 in the corresponding subnet (i.e. that LAN-in has 192.168.1.165 as an IP address, and LAN-out has 192.168.253.165 as an IP address), while "Southwest" has the end number 166 and "East" the end number 164.



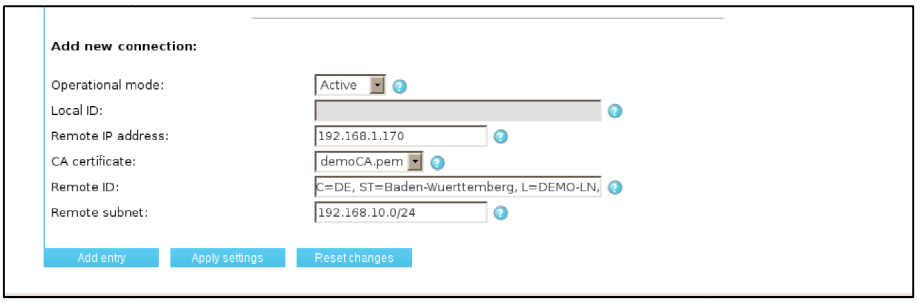
The configuration for "West" ("Southwest" is configured in the same way) looks as follows:



Configuration for "East":

The settings for the local IPsec endpoint and the authentication method are the same for all connections, and are defined above the table. The local interface describes the actual tunnelling endpoint. The entire traffic from or to the specified local subnet is encrypted or decrypted there (The packets which originate from the firewall will be encrypted if no subnet is specified.). If the remote terminal cannot directly be reached (e.g. if access is gained via a router), it might be required for IPsec to explicitly specify the address of the next router (Usually, this box should remain empty though.). If *Use default route* is clicked, the default gateway specified in the IP configuration is used as the next router.

Underneath the table, new connections can be added, for instance:



© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

The operating mode of a connection is either Active (connection is immediately established) or Passive (waiting for inbound connections). Instead of an IP address, a host name might be used as well. If the subnet box is left blank, the packets of the firewall are encrypted (like with the local subnet).

If certificates are used for authentication, the CA certificate, against which the certificate of the remote terminal is to be verified, and the subject field of the remote terminal certificate must be specified as the Remote ID for this connection ("West" uses, for instance demo-client2.pem in order to authenticate itself, expects that the certificate is signed by the demoCA.pem CA and has the *C=DE, ST=Baden-Wuerttemberg, L=DEMO-LN1, O=DEMO-ON1, OU=DEMO-OUN1, CN=DEMO-CN1, emailAddress=demo1@ads-tec.de subject line information,* which corresponds with demo-client1.pem of "East"). The subject field can simply be copied from another firewall from the Certificates page by using "copy & paste":



Note:

The subject field information must exactly match the certificate description of the remote terminal.

Should a router use NAT between both firewalls (i.e. change the IP addresses of packets, like a router does, which connects a LAN with the Internet), the NAT Traversal option must be set (since authentication might fail otherwise).

If the network performance decreases due to NAT, it might help to restrict the Maximum Transfer Unit (MTU) number.

For security reasons, certificates are usually sent on request only. But this might prevent compatibility with some providers, like for instance with Cisco and Safenet, under certain circumstances. That means if a firewall is to be connected with a device of such a provider, the Send certificates option must probably set to Always.

If a firewall is to be connected with a device which is only capable of non-secure methods (DES/DH1), the Allow weak encryption option must be enabled.

The subnets must be different, in order to allow IPsec service to route the packets in an unambiguous way. That means that an individual virtual LAN is not established, but the data traffic between different subnets is secured.

If a PSK is used for authentication, the Remote ID box might be left blank (The IP address is then used as an ID.). If the remote terminal, however, explicitly uses a defined ID (for instance a Cisco router), it might be required to specify this ID.

Should the authentication method change, the invalid entries will be labelled as such, and not considered until the method is changed back again.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

"ROADWARRIOR" SERVER CONFIGURATION

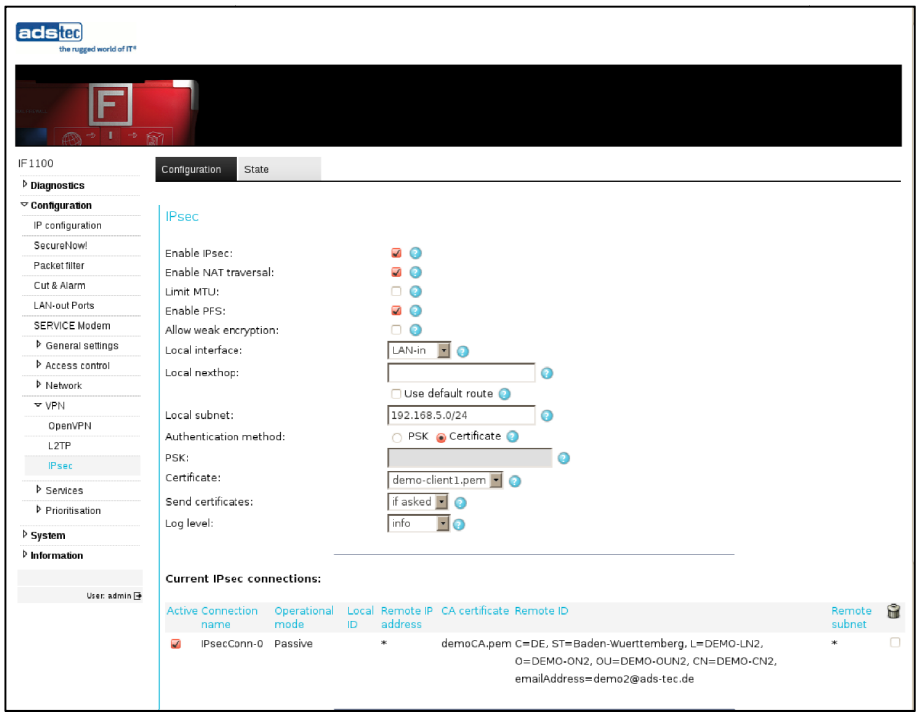
Exactly one specific connection (the so-called roadwarrior connection) may be defined by setting the IP address and the subnet of the remote terminal to "*". Even if this is not a server mode in its usual sense, it can be designated as such, because the firewall has to await (passively) the roadwarrior activity (i.e., the Passive operating mode is required). Any number of roadwarriors is allowed to connect (only if authentication is successful, of course).

In this example, a "Roadwarrior" firewall behind a router called "Router" connects with a "Gateway" firewall, which is configured as a roadwarrior server and routes the traffic into a local network:



Whilst you must know the certificate subject info in the "Subnet-to-subnet" use case in detail, a * might be used as a wildcard character for entries in the roadwarrior setup, which are allowed to have any value (e.g. C=DE and all other entries set to * means that the country must be Germany, but that the other entries might have any possible value). Even if wildcards are allowed, all subject info boxes must exist and must match the certificates of the roadwarrior, as well as must be sorted, because otherwise authentication might fail (If e.g. an email address stands as the last entry in the subject info box of the roadwarrior certificate, and if the firewall is usually not supposed to verify it, the last entry in the certificate subject info of the firewall must be "emailAddress=*", and cannot be omitted).

The configuration of the "Gateway" device looks as follows:



Note:

*Although * may be used as a wildcard for any box in the certificate subject info, all box entries must always exist and match the certificates of the roadwarriors.*

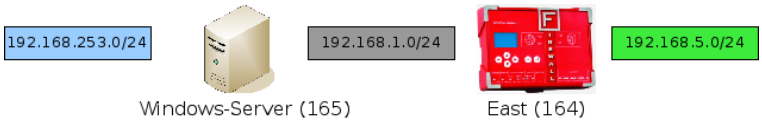
The email address box has three equivalent notations: E=, emailAddress=*, and Email=*.*

The NAT traversal option should always be enabled, since you don't know beforehand, if a roadwarrior is located behind a NAT router (e.g. one that has no direct connection with the Internet, but is connected with the Internet via a router). This option has no effect if NAT traversal is not required.

Should the roadwarrior connect from inside a LAN by using a NAT router, the LAN subnet must belong to one of the official IP address ranges for private networks, i.e. to 10.0.0.0/8, 192.168.0.0/16 or 172.16.0.0/12.

"SUBNET-TO-SUBNET" CONFIGURATION BETWEEN A WINDOWS 2003 SERVER AND A FIREWALL

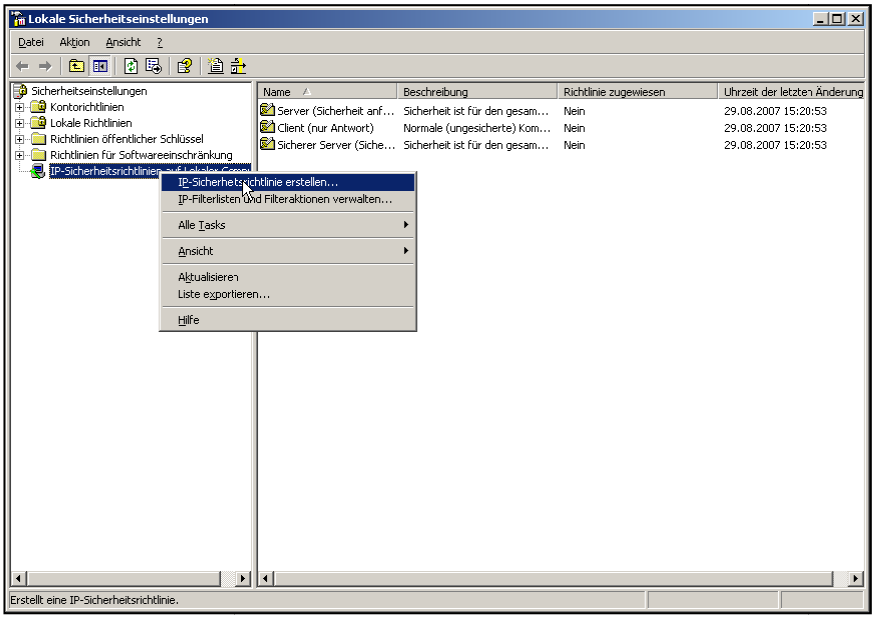
A corresponding IP security policy must be created under Windows, in order to establish an IPsec tunnel connection between a Windows server and a firewall. The exemplary setup corresponds with the "Subnet-to-subnet" example, with the difference that the Windows server is used instead of the "West" device and that "Southwest" is omitted. The "East" device configuration is unchanged (the connection for "Southwest" is simply no longer used):



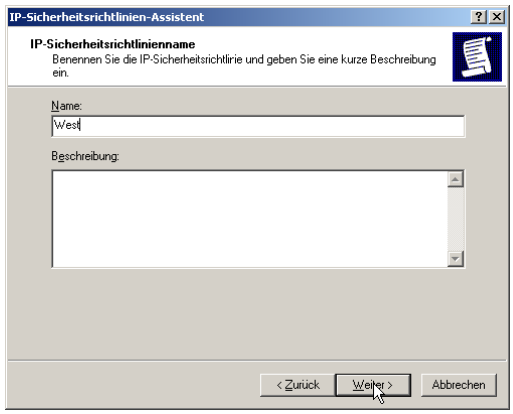
That means the Windows server has 192.168.253.165 as the internal, and 192.168.1.165 as the external IP address; it authenticates itself by using the demo-client2.pem certificate (You'll find a detailed instruction for importing this certificate into the certificate memory in the "Certificates" use case.).

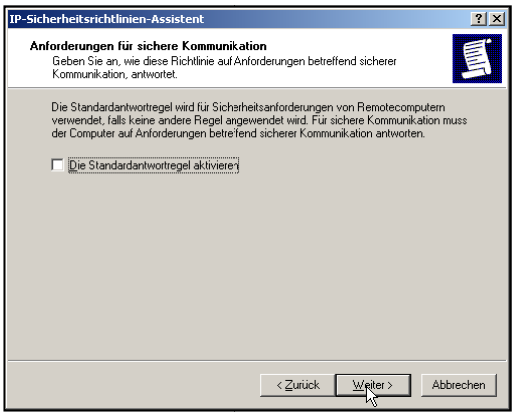
First, you'll have to start the Microsoft Management Console in order to create a new IP policy. To do this, enter the secpol.msc command in the "Start/Run..." line. This wizard is started by right-clicking on IP security policies on Local computer, and by clicking there on Create IP security policy.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

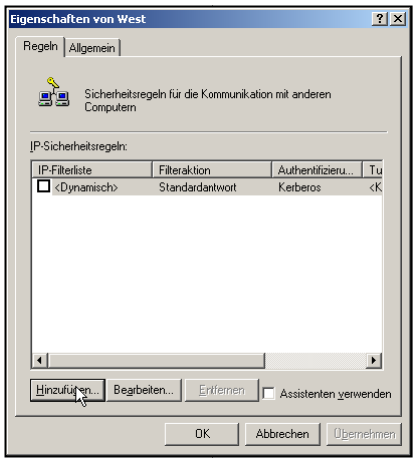


A name (e.g. "West") must be specified for this policy, and the Default response policy must be disabled:

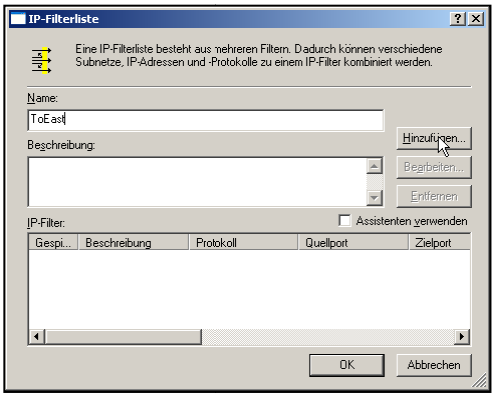



IP-Sicherheitsrichtlinien-Assistent
Anforderungen für sichere Kommunikation
Geben Sie an, wie diese Richtlinie auf Anforderungen betreffend sicherer Kommunikation, antwortet.
Die Standardantwortregel wird für Sicherheitsanforderungen von Remotecomputern verwendet, falls keine andere Regel angewendet wird. Für sichere Kommunikation muss der Computer auf Anforderungen betreffend sicherer Kommunikation antworten.
Die Standardantwortregel aktivieren
< Zurück
Weiter >
Abbrechen

If you leave the Edit properties box ticked when finishing, the Properties dialogue will immediately be opened (Otherwise go to the respective policy by right-clicking it and use Select properties). For each direction of the IPsec tunnel a separate policy must be defined. In order to do so, untick the Use wizard box and click the Add button:

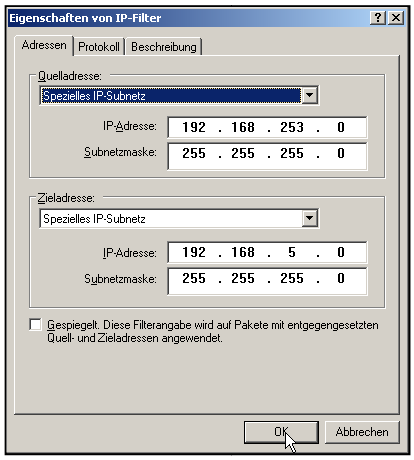


Click on Add in the active "IP filter list" tab in order to create a new filter list. This list is to be used for the outbound traffic (Use e.g. "ToEast" as a name), and requires exactly one filter policy. In order to create this list, you'll have to disable Use wizard and then to click on Add:

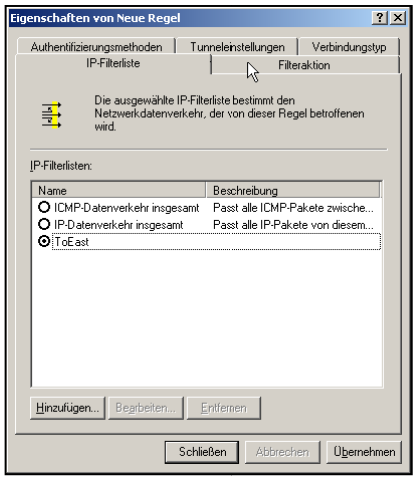


© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

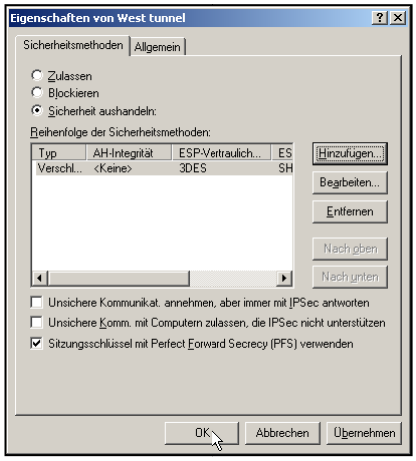
The own internal subnet (192.168.253.0/24) is used as the Source address, and the internal subnet of the firewall (192.168.5.0/24) is used as the Destination address. The Protocol type in the Protocol tab must be set to "Any". The option "Mirrored" should not be ticked (disabled):



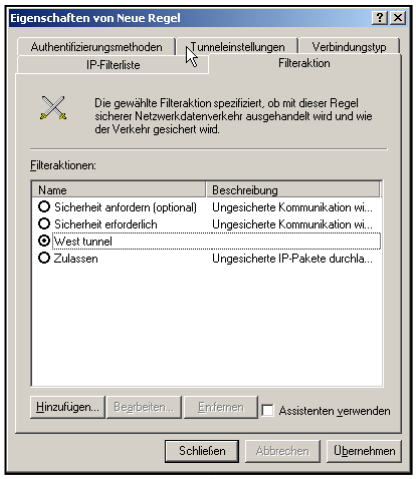
Push the OK button twice in order to return to Properties of the policy. The filter must be enabled by clicking the round radio button in front of it:



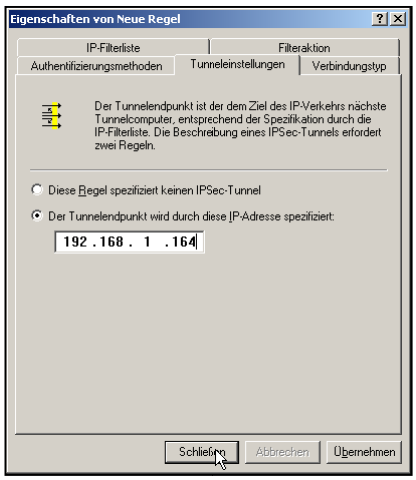
Then switch to the Filter action tab. Disable the wizard there once more and click on Add. In this case, the IPsec tunnel must be established as the relevant action for data traffic between both subnets. In order to do so, select Negotiate security level and click on Add. Select Encryption and Integrity as the method, and push the OK button. Perfect-Forward-Secrecy must be enabled, whereas Insecure communication must be disabled. The action can be renamed under General (e.g. to "West tunnel"):



This action must, like the filter, also be selected by clicking the radio button:

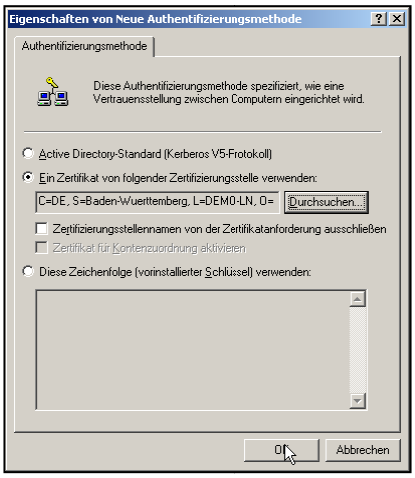


Switch to the Tunnel settings tab next and specify the external IP address of the firewall as the tunnel endpoint:

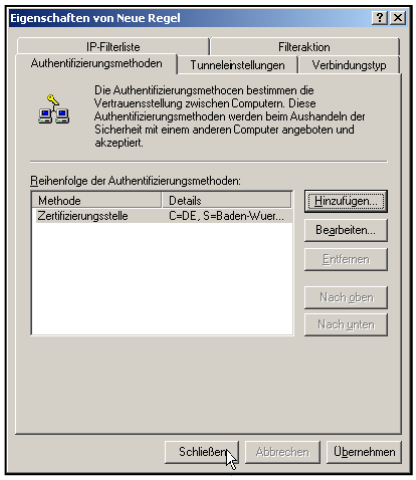

Eigenschaften von Neue Regel
IP-Filterliste
Filteraktion
Authentifizierungsmethoden
Tunneleinstellungen
Verbindungstyp
Der Tunnelendpunkt ist der dem Ziel des IP-Verkehrs nächste Tunnelcomputer, entsprechend der Spezifikation durch die IP-Filterliste. Die Beschreibung eines IPSec-Tunnels erfordert zwei Regeln.
Diese Regel spezifiziert keinen IPSec-Tunnel
Der Tunnelendpunkt wird durch diese IP-Adresse spezifiziert:
192 . 168 . 1 . 164
Schließen
Abbrechen
Übernehmen

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

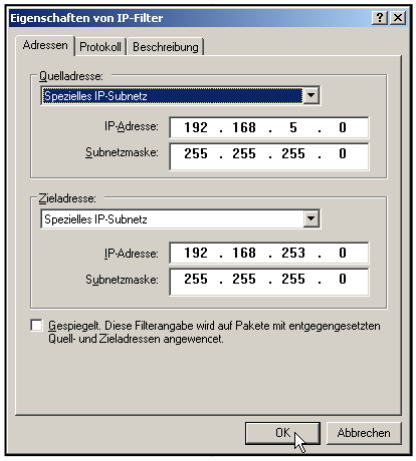
Finally, you'll have to unselect "Active Directory Standard (Kerberos V5 protocol)" method) in the Authentication methods tab, and click on Add. Click in this place on "Use a certificate from the following certification authority", and select the "DEMO-CN" certification authority:

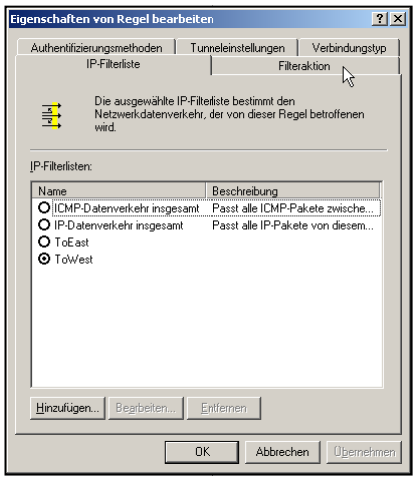


The All network connections item should be selected in the Connection type tab. Defining this policy is finished by using Close:

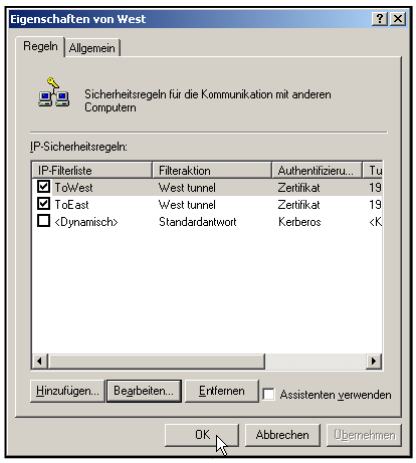


In the next step, the policy for the inbound traffic must be defined under Policies in the same way. Click once more on Add, create a new IP filter list for the opposite direction of the "ToEast" filter (e.g. using "ToWest" as a name) and select it:



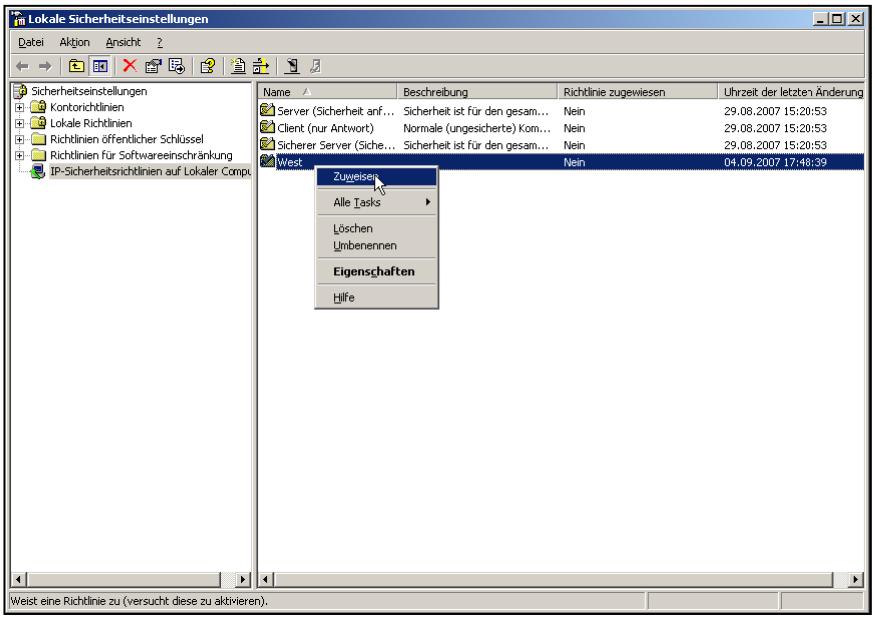


The West tunnel action must again be selected in the Filter action tab. The external IP address of the Windows server (192.168.1.165) must be specified as the tunnel endpoint in the Tunnel settings tab. The same settings as with the "ToEast" policy must be made in the Authentication methods tab. Both rules, the "ToEast" and the "ToWest" rule, are then the only active rules in this policy:

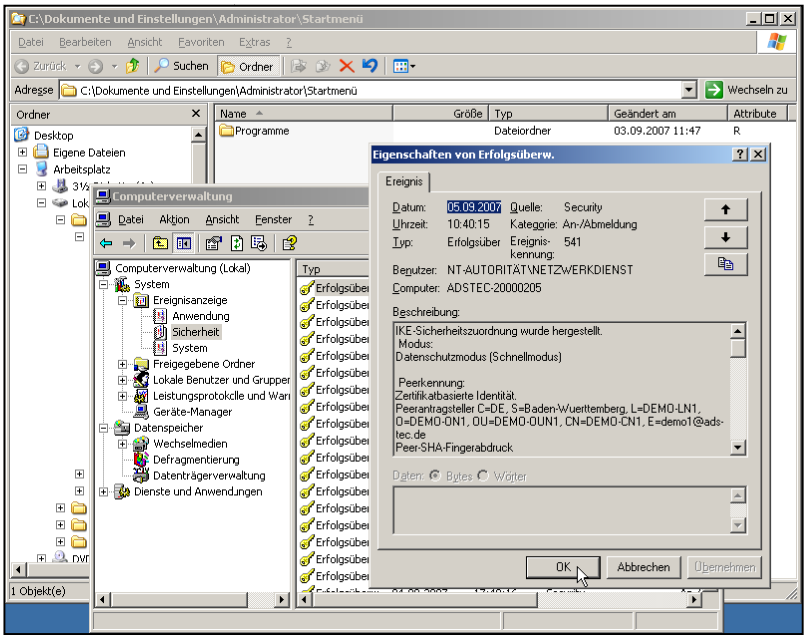


© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

Subsequently, push the OK button in order to return to the console. Finally, the policy must be enabled. In order to do that, right-click on the respective policy, which opens the menu and click there on Assign:

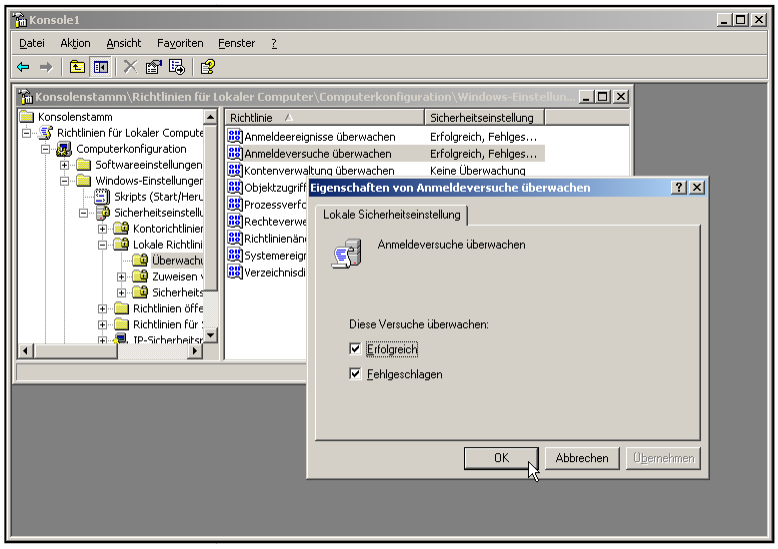


In the Computer management (Open Explorer, right-click on My Computer and then on Manage), you can view messages with respect to IPsec under Event viewer/Security:



If the tunnel was properly established, one message each must be available for the Main mode and for the Quick mode, which indicates that the IKE security assignment was established. In order to get also messages for failed connection attempts, you'd have to start the Microsoft management Console first by using "Start/Run..." and entering mmc in the command line; then you'd have to add the "Group-policy object editor" snap-in there.

There, you'd have to tick the "Failed" box under Policies for Local computer/Computer configuration/Windows settings/Security settings/Local policies/Monitoring policies in the Properties for "Monitor login events" and "Monitor login attempts":



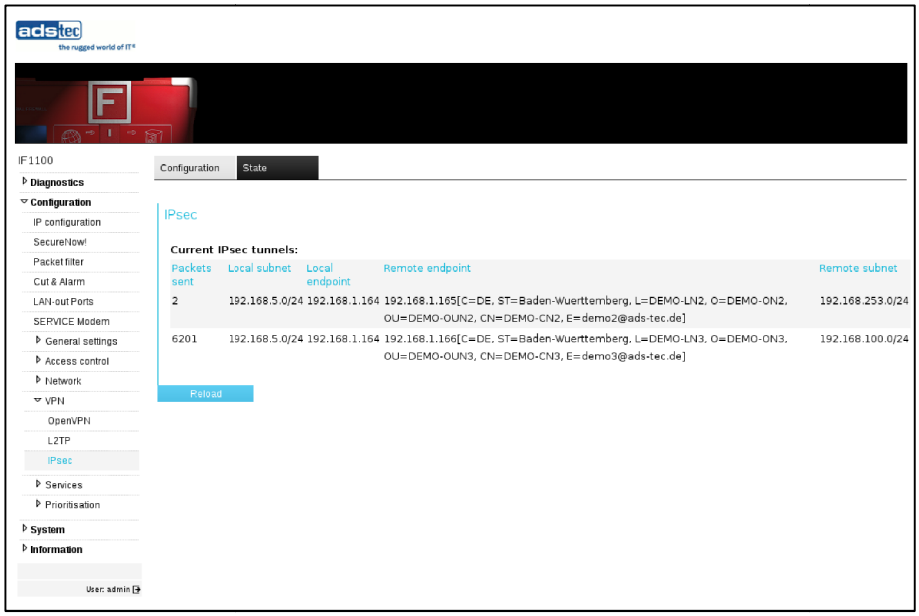
Note:

You'll find a complete documentation with respect to IPsec for Windows 2003 server at http://support.microsoft.com/kb/816514/EN-US.
Please refer to the "Certificates" use case if you'd like to import certificates.
The demo-client2.pem certificate cannot directly be selected. The Windows server will test all certificates of the specified certification authority until authentication is successful.
Should the server be part of a domain with previously set security policies, a new Organisation unit must be created in Active Directory (with the server as a member), and must be assigned to the security policy.
The route to the internal subnet of the firewall must probably be set manually. In the above example this is achieved, because the external network adapter of the server uses the external IP address of the firewall (192.168.1.164) as the default gateway.
If the Windows server is supposed to exclusively permit traffic between both subnets, further filter rules must be created in order to prevent traffic from or to other subnets.
Establishing an IPsec tunnel connection between a PC using Windows XP Professional and the internal network of a firewall is done in the same way. The only difference in this case is, that "Use own IP address" must be specified as the Source address of the "ToEast" filter list and as the Destination address of the "ToWest" filter list. However, it is more useful to use L2TP in this use case (which uses IPsec as a basis), because it can be configured easier. With respect to this, please refer to our use case "L2TP".
It is not recommended to edit filter rules by using remote access. It is possible that you can no longer reach the system if an error occurs during this process.
Information and statistics with respect to IPsec may be retrieved in the IP security monitor MMC snap-in.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

IPSEC STATUS PAGE

Active tunnels, that means only actually present IPsec connections, are displayed on the IPsec status page. This display does not indicate to which defined connection the tunnel belongs (but the assignment is visible in the configuration page table). See here for instance, for the firewall "East" from the "Subnet-to-subnet" example:



Note:

Although the remote terminal was authenticated, the tunnel could not properly be established, if the remark "hold" or "trap" is found next to the number of transmitted packets. This indicates a configuration issue (e.g. wrong subnet setup).

REGULAR IPSEC EVENTLOG MESSAGES

The IPsec tunnel is established in two phases, as was mentioned at the start. First, both parties must authenticate (Main mode), and then the actual tunnel is established (Quick mode). A successful connection establishment generates for the "Subnet-to-subnet" scenario for the "West" device, for instance, the following Eventlog entries (read from top to bottom):

IF1xxx ipsec_pluto[1677]: "IPsecConn" #3: ISAKMP SA established

IF1xxx ipsec_pluto[1677]: "IPsecConn" #3: no crl from issuer "C=DE, ST=Baden-Wuerttemberg, L=DEMO-LN, O=DEMO-ON, OU=DEMO-OUN, CN=DEMO-CN, E=democa@ads-tec.de" found (strict=no)

IF1xxx ipsec_pluto[1677]: "IPsecConn" #3: peer ID is 'C=DE, ST=Baden-Wuerttemberg, L=DEMO-LN1, O=DEMO-ON1, OU=DEMO-OUN1, CN=DEMO-CN1, E=demo1@ads-tec.de'

IF1xxx ipsec_pluto[1677]: "IPsecConn" #3: responding to Main Mode

IF1xxx ipsec_pluto[1677]: "IPsecConn" #2: IPsec SA established

IF1xxx ipsec_pluto[1677]: "IPsecConn" #2: initiating Quick Mode {using isakmp#1}

IF1xxx ipsec_pluto[1677]: "IPsecConn" #1: ISAKMP SA established

IF1xxx ipsec_pluto[1677]: "IPsecConn" #1: no crl from issuer "C=DE, ST=Baden-Wuerttemberg, L=DEMO-LN, O=DEMO-ON, OU=DEMO-OUN, CN=DEMO-CN, E=democa@ads-tec.de" found (strict=no)

IF1xxx ipsec_pluto[1677]: "IPsecConn" #1: peer ID is 'C=DE, ST=Baden-Wuerttemberg, L=DEMO-LN1, O=DEMO-ON1, OU=DEMO-OUN1, CN=DEMO-CN1, E=demo1@ads-tec.de'

IF1xxx ipsec_pluto[1677]: "IPsecConn" #1: initiating Main Mode

IF1xxx ipsec_pluto[1677]: loaded private key file 'demo-client2.key' (497 bytes)

IF1xxx ipsec_pluto[1677]: loaded host cert file 'demo-client2.pem' (1384 bytes)

IF1xxx ipsec_pluto[1677]: loaded CA cert file 'demoCA.pem' (1330 bytes)

IF1xxx ipsec_pluto[1677]: Starting IPsec service

ISAKMP SA established means that authentication was successful, and **IPsec** SA established means that the tunnel was successfully established. If both parties are set to Active (like in above example), it is possible that both the authentication and the tunnel establishment occur twice. In an Active/Passive constellation this would happen only once. Authentication and tunnel establishment are repeated in varying time intervals in order to increase security.

IPSEC EVENTLOG ERROR MESSAGES

In general it can be said that errors in the Main mode indicate failed authentication (Either the remote terminal was not reached, or one of both parties couldn't authenticate itself properly.). Errors in Quick mode, on the other hand, indicate erroneous configuration of the tunnel endpoints (a wrong subnet specification, for example). A few error messages are listed below.

The certificate, by means of which the firewall is trying to authenticate, is invalid, because the system time is not included in the range of the validity period. As a result, the certificate cannot be used and the firewall cannot authenticate:

IF1xxx ipsec_pluto[3161]: "IPsecConn" #1: sending encrypted notification INVALID_KEY_INFORMATION to 192.168.1.164:500

IF1xxx ipsec_pluto[3161]: "IPsecConn" #1: no RSA public key known for 'C=DE, ST=Baden-Wuerttemberg, L=DEMO-LN1, O=DEMO-ON1, OU=DEMO-OUN1, CN=DEMO-CN1, E=demo1@ads-tec.de'

IF1xxx ipsec_pluto[3161]: "IPsecConn" #1: X.509 certificate rejected

IF1xxx ipsec_pluto[3161]: "IPsecConn" #1: checking validity of "C=DE, ST=Baden-Wuerttemberg, L=DEMO-LN1, O=DEMO-ON1, OU=DEMO-OUN1, CN=DEMO-CN1, E=demo1@ads-tec.de": X.509 certificate is not valid until Jan 11 12:59:20 UTC 2007 (it is now=Dec 31 23:01:39 UTC 2006)

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

The remote terminal cannot be reached (not available):

IF1xxx ipsec_pluto[9224]: "IPsecConn" #1: ERROR: network error on LAN-in (sport=500) for message to 192.168.1.168 port 500 , complainant 192.168.1.165: No route to host

The remote terminal can be reached, but either the IPsec service does not run there at all or it was configured for another interface:

IF1xxx ipsec_pluto[3609]: "IPsecConn" #23: ERROR: network error on LAN-in (sport=500) for message to 192.168.1.165 port 500 , complainant 192.168.1.165: Connection refused

The remote terminal does not accept the desired type of authentication (PSK or certificates):

IF1xxx ipsec_pluto[4186]: packet from 192.168.1.164:500: received notification NO_PROPOSAL_CHOSEN

The remote terminal tries to authenticate by using a certificate, although a PSK is expected:

IF1xxx ipsec_pluto[4186]: "IPsecConn" #6: sending notification NO_PROPOSAL_CHOSEN to 192.168.1.164:500

IF1xxx ipsec_pluto[4186]: "IPsecConn" #6: policy does not allow OAKLEY_RSA_SIG authentication

The remote terminal tries to authenticate by using a PSK, although a certificate is expected:

IF1xxx ipsec_pluto[1664]: "IPsecConn" #59: sending notification NO_PROPOSAL_CHOSEN to 192.168.1.165:500

IF1xxx ipsec_pluto[1664]: "IPsecConn" #59: policy does not allow OAKLEY_PRESHARED_KEY authentication

The PSK of both parties do not match:

IF1xxx ipsec_pluto[4186]: "IPsecConn" #16: sending notification PAYLOAD_MALFORMED to 192.168.1.164:500

Authentication at the remote terminal failed. The corresponding "sending notification" message of the other party stands there usually in the context of explanatory error messages:

IF1xxx ipsec_pluto[1664]: "IPsecConn" #54: received notification INVALID_ID_INFORMATION

The certificate subject info of the remote terminal does not match the expected certificate subject info, and will thus be rejected (e.g. the state of "Berlin" is expected, but the certificate originates from the state of "Baden-Württemberg", according to the subject info):

IF1xxx ipsec_pluto[7061]: "IPsecConn" #1: we require peer to have ID 'C=DE, ST=Berlin, L=DEMO-LN1, O=DEMO-ON1, OU=DEMO-OUN1, CN=DEMO-CN1, E=demo1@ads-tec.de', but peer declares 'C=DE, ST=Baden-Wuerttemberg, L=DEMO-LN1, O=DEMO-ON1, OU=DEMO-OUN1, CN=DEMO-CN1, E=demo1@ads-tec.de'

The equivalent message, if the firewall responds to a request from a remote terminal, instead of having initiated the authentication process on its part, (in this example the

remote terminal offers a certificate from Baden-Württemberg, although the connection is only defined for a certain certificate from Berlin) is:

IF1xxx ipsec_pluto[7061]: "IPsecConn" #2: no suitable connection for peer 'C=DE, ST=Baden-Wuerttemberg, L=DEMO-LN1, O=DEMO-ON1, OU=DEMO-OUN1, CN=DEMO-CN1, E=demo1@ads-tec.de'

Authentication was successful, but the definition of tunnelling endpoints does not match (In this example, the remote terminal expects the 192.168.6.0/24 subnet, although 192.168.5.0/24 was specified as the local subnet.):

IF1xxx ipsec_pluto[4707]: "IPsecConn" #1: cannot respond to IPsec SA request because no connection is known for 192.168.6.0/24===192.168.1.164[C=DE, ST=Baden-Wuerttemberg, L=DEMO-LN1, O=DEMO-ON1, OU=DEMO-OUN1, CN=DEMO-CN1, E=demo1@ads-tec.de]...192.168.1.165[C=DE, ST=Baden-Wuerttemberg, L=DEMO-LN2, O=DEMO-ON2, OU=DEMO-OUN2, CN=DEMO-CN2, E=demo2@ads-tec.de]

If the SERVICE tunnelling endpoint interface is selected and the modem connection is not yet active at this point in time, establishing the IPsec connection will be postponed until the SERVICE interface is actually started up:

IF1xxx ipsec_pluto: IPsec service not started yet: SERVICE is not running

This message indicates an internal IPsec configuration error:

ipsec_pluto[1677]: packet from 192.168.11.166:500: initial Main Mode message received on 192.168.11.164:500 but no connection has been authorised==192.168.253.0/24

IPSEC FILTER RULES

If IPsec is enabled, the IPsec version of the tunnel interface additionally appears in the packet filter (e.g. there will be LAN-In (IPsec) additionally to LAN-In). This version may then be used for defining rule sets for the data traffic through the IPsec tunnel. The regular version continues referring to the remaining data traffic.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

IPSEC SPECIFICATION

Key exchange	IKE (Internet Key Exchange) is based on the ISAKMP (Internet Security Association and Key Management Protocol).
IKE phases	Main mode Quick mode
Authentication method	X.509 certificates incl. RSA PSK
DH groups	DH group 1 MODP 768 DH group 2 MODP 1024 DH group 5 MODP 1536
Data integrity	MD5 (128bit) SHA1 (160bit)
Encryption	DES (64bit) 3DES (192bit) AES (128bit) AES (192bit) AES (256bit)
Hardware encryption	Yes
IPsec mode	ESP tunnel
Maximum number of IPsec connections	64
NAT traversal	Yes
Dead peer detection	Yes

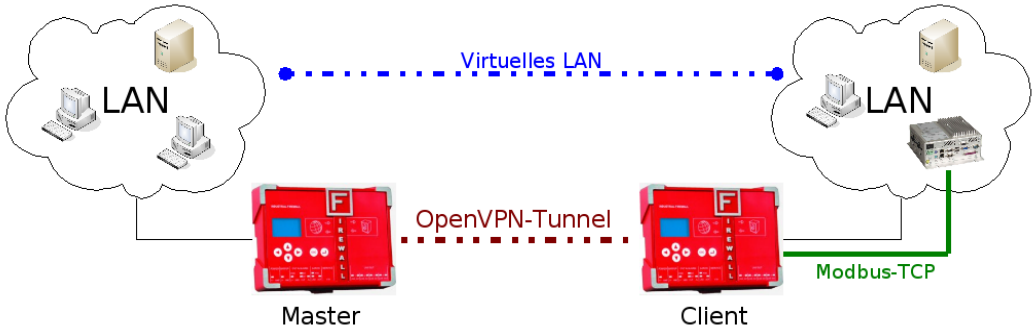
The firewall is using AES128-MD5-DH2 in the Main mode and AES128-SHA1 in the Quick mode, by default.

11.13 MODBUS TCP

GENERAL

Modbus TCP allows the control of the function of a device via Ethernet from a PLC unit, as well as the retrieval of status information. Communication services (SERVICE, IPsec and OpenVPN) can be controlled at the firewall and CUT&ALARM messages can be acknowledged by using this protocol.

If, for example, an OpenVPN connection is defined between two firewalls, and the client is configured to be "inactive" (see the "OpenVPN" use case for that), then the client can be activated from a PLC unit via Modbus TCP and the OpenVPN connection be established in this way.

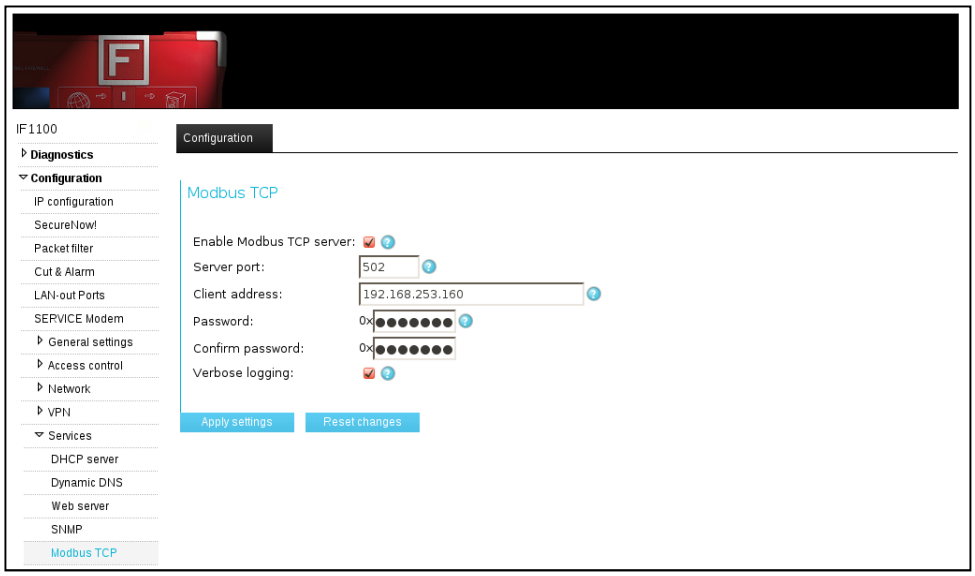


Note:

Only one PLC can make a connection with the Modbus TCP server of the firewall at the same time.
You'll find a detailed definition of registers in the "IF1xxx Modbus TCP register overview" document.
The general registers (version, password high, password low), the status register and the CUT&ALARM input register can be addressed at any time (but the status register in read-only mode, only).
The SERVICE input register can only be addressed if the SERVICE interface is enabled (you can then make a dial-in connection or terminate a connection via Modbus TCP).
The IPsec input register always enables or disables the entire service, which means that all defined and enabled connections are enabled or disabled at once. Connections with an active mode will automatically establish the connection, whereas connections with a passive mode will await a connection request. Managing these connections individually is impossible.
An OpenVPN input register can only be addressed if the corresponding entry is defined (you can then activate and deactivate this entry via Modbus TCP). In this case, not the list position but the associated L2-VPN interface counts. So, if for instance the relevant entry is associated with the L2-VPN3 interface, the status register and the input register for OpenVPN-3 must be used.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

MODBUS TCP CONFIGURATION



The Modbus TCP server can be enabled under Configuration/Advanced/Modbus TCP. Additionally, the following settings can be made:

There are no restrictions for selecting the server port. If a certain port was specified, the firewall waits for incoming requests on the default port for Modbus TCP (502).

Access can be limited to a certain client. For this purpose, the client address may be specified as an IP address on the one hand, or as a host name, which will be resolved when starting up the server, on the other hand. The connection can be established from any computer if no specific client address is specified.

For increasing the security, a 32 bit password may be specified. Before a client is allowed to access the status and input registers, the client has to write the 16 high-order bits into the "PASSWORD-HIGH" register 0x01 and the 16 low-order bits into the "PASSWORD-LOW" register 0x02 if a password is set up. Otherwise the client has direct access to all registers.

Usually only access violations are reported (if the IP address is restricted or a password is required), so that the Eventlog is not overflowing with information. If "Message details" is activated, additional information about connection establishment, requests and access times will be logged.

Note:

The password is checked when the low-order portion is written in register 0x02. So, if the password is 0xaa11bb22 for example, then 0xaa11 must first be written in register 0x01, and 0xbb22 in register 0x02, subsequently. The password is valid for the duration of the TCP connection. If the connection is re-established, all password registers are reset to 0x0000.

If a host name is used for restricting the client address, this name will be resolved into an IP address as early as during the server start, and not only when the actual connection is established. This means that Modbus TCP has to be restarted if the meaning of a host name changes.

ACTIVATING OPENVPN

In order to enable an OpenVPN entry associated with the L2-VPN1 OpenVPN interface for example, the PLC must set the 0x24 register of unit 0x00 to 1 by using the 0x10 function code (write multiple registers). If this register is set to 0, the entry is disabled and the connection shut down.



Note:

Unit 0 stands for the firewall itself and is the only permitted unit.

The connection is directly established and lasts for approximately 10 seconds. This is the time needed for responding to the request. This means the PLC receive timeout must be set sufficiently high.

The input register contains the most recently written value regardless of which result the action had (or 0 if the input register has not been written yet). The actual connection status must be read from the corresponding status register (for example 0x14 for OpenVPN-1).

The other input registers work in the same way (except for the 0x10 CUT&ALARM register, which can only be set to 0x00 for acknowledging the message). Please refer to the "IF1xxx Modbus TCP register overview" document for a detailed description of input registers.

READING THE STATUS REGISTERS

The PLC is able to retrieve all status registers in one request. For this purpose, it has to read 14 registers from the starting address 0x10 of unit 0x00 by using the function codes 0x03 or 0x04.



Note:

The reading of all status registers takes approximately 5 seconds. Due to performance reasons the status registers should not be read too often (once per minute at most). You'll find a detailed explanation of the register contents in the "IF1xxx Modbus TCP register overview" document.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

11.14 IF1000 SERIES MODBUS TCP REGISTER OVERVIEW

GENERAL

Modbus TCP implementation is based on the official documentation of the Modbus-IDA Independent User Organization (http://modbus.org):

- http://www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf
- http://www.modbus.org/docs/Modbus_Messaging_Implementation_Guide_V1_0b.pdf

A Modbus TCP server runs on IF1xxx, which receives the requests on TCP port 502 (if not otherwise configured). Currently, only the logical unit 0 can be addressed, which stands for the firewall itself.

The Modbus TCP server is able to process the following address codes:

- 0x03 (Read Holding Registers)
- 0x04 (Read Input Registers)
- 0x10 (Write Multiple Registers)

Reading operations 0x03 and 0x04 are identical in their behaviour. In the following explanations, bit 0 stands for the lowest and bit 15 for the highest bit in the order used in the registers.

If an error occurs whilst processing the request, the following exception codes are possible:

0x01	Invalid function code	Neither 0x03, 0x04, nor 0x10 was used as a function code.
0x02	Invalid register	The register either does not exist, or the desired operation cannot be performed.
0x03	Invalid register value	The value to be written is invalid for the register.
0x04	Server error	An internal error occurred while processing the request.

Note:

Processing time for implementation has not been optimised. Establishing an OpenVPN connection, for instance, may take approximately 10 seconds. Reading of all status registers in a request may take approximately 5 seconds. The response from the Modbus TCP server requires a corresponding period of time. For performance reasons, these requests thus may not be performed too often (The status in particular should only be retrieved once per minute at most, and should be restricted to required registers), and the PLC timeouts should be sufficiently high. Furthermore, only one client at a time may connect to the firewall using the Modbus TCP server.

REGISTER OVERVIEW

General registers:

- 0x00 (VERSION)
- 0x01 (PASSWORD-HIGH)
- 0x02 (PASSWORD-LOW)

Status registers:

- 0x10 (CUT&ALARM)
- 0x11 (SERVICE)
- 0x12 (reserved for L2TP)
- 0x13 (IPsec)
- 0x14 (OpenVPN-1)
- …
- 0x1D (OpenVPN-10)

Input registers:

- 0x20 (CUT&ALARM)
- 0x21 (SERVICE)
- 0x22 (reserved for L2TP)
- 0x23 (IPsec)
- 0x24 (OpenVPN-1)
- …
- 0x2D (OpenVPN-10)

Status registers cannot be written. The content for all status registers for a specific connection is similar:

- Bit 0 contains the information whether the considered connection is defined at all, i.e. whether there is an entry or the service is enabled.
- Bit 1 contains the information whether the connection was enabled. For SERVICE, this bit is only temporarily set, as long as the dialling process runs, and with IPsec it is always set if the mode is "active" or "passive" (that means if the connection cannot manually be controlled at all).
- Bit 2 contains the information whether this connection is actually existent.
- The other bits indicate type specific information.

"Read" as well as "Write" are permitted actions for the input registers. As long as the corresponding service of a register for a specific connection is not active or cannot be configured, all writing attempts will be invalid and the exception code 0x02 (invalid register) will be returned. Independent on the success of an action initiated by writing an input register, the value will be written into the input register and can be retrieved. However, the actual status of the corresponding service must be retrieved from the status register.

VERSION (0X00 REGISTER)

This register is currently always set to 0x0100, and you read it but not write it. The higher value byte is the major, and the lower value byte is the minor version number.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

PASSWORD (0X01 AND 0X02 REGISTER)

Register 0x01 (PASSWORD-HIGH) is the high-order portion and register 0x02 (PAASWORD-LOW) the low-order portion of the 32 bit password. Both registers may be written and read as usual. If a password is required, it must be set correctly before you can access the status and input registers. The password verification is carried out as soon as register 0x02 is written (because of that, register 0x01 must be set first). The password is valid for the entire duration of the TCP connection. If the connection is re-established, the content of both registers is reset to 0.

CUT & ALARM

Status (0x10 register)

Bits	Meaning	Explanation
0	ALARM	ALARM is active
1	Internal CUT	CUT is active
2	External CUT	CUT is active
3-15	Unused	

Input (0x20 register)

The register can be written with the value 0x0000 in order to acknowledge ALARM and internal CUT messages. The external CUT cannot be reset in this way because it is a signal that is externally applied. 0x0000 is the only permitted value.

SERVICE

Status (0x11 register)

Bits	Meaning	Explanation
0	Service active	The service is enabled
1	Dial-in	SERVICE attempts to connect to a remote terminal (Dial-out only)
2	Connected	SERVICE is connected with a remote terminal
3	Dial-out	SERVICE is configured as Dial-out (if not set, then configured as Dial-in)
4-15	Unused	

Input (0x21 register)

This register can either be written with the value 0x0001 (establish the connection, for Dial-out only) or with the value 0x0000 (shut down connection).

L2TP

[RESERVED]

IPSEC

Status (0x13 register)

Bits	Meaning	Explanation
0	Service active	The IPsec service is enabled and the connection configured as manual
1	Enabled	The connection is enabled (always with Active/Passive)
2	Connected	Tunnel is established
3	Manual mode	Connection can explicitly be established/shut down
4	Active	Mode if the connection cannot be operated in manual mode (if not set up: Passive)
5	Dynamic remote terminal	Connection awaits roadwarriors (i.e. multiple connections are possible)
6-7	Unused	
8-15	Roadwarriors	Number of roadwarriors

Bits	Meaning	Explanation
0	Defined	At least one connection is defined
1	Enabled	IPsec is globally enabled
2	Connected	At least one tunnel is established
3-7	Unused	
8-15	Enabled tunnels	How many IPsec tunnels are actually established

Input (0x23 register)

This register can either be written with the value 0x0001 (establish the connection), or with the value 0x0000 (shut down connection). This is impossible for versions before version 1.0, if IP sec is configured for manual control.

OPEN VPN

Status (0x14-0x1D register)

Bits	Meaning	Explanation
0	Defined	The OpenVPN entry exists
1	Enabled	OpenVPN entry is enabled
2	Connected	Tunnel is established
3	Server	The entry is defined as a Server
4-7	Unused	
8-15	Clients	Number of clients (with Server only)

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

Input (0x24-0x2D register)

This register can either be written with the value 0x0001 (enable entry) or with the value 0x0000 (disable entry) if this entry is defined.

11.15 SIM CARD

GENERAL

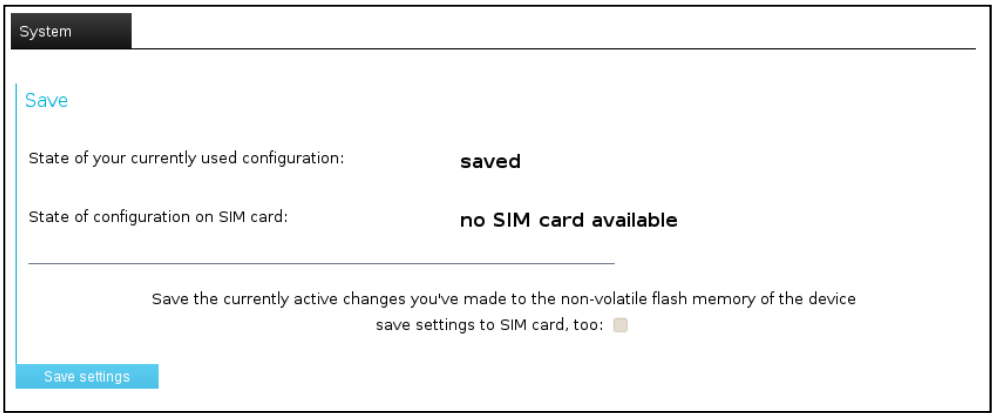
A faulty piece of equipment may be simply replaced by using a SIM card. You just have to remove the SIM card from the faulty device and insert it in the replacement device. No intervention by qualified staff is required.

SIM CARD TYPE

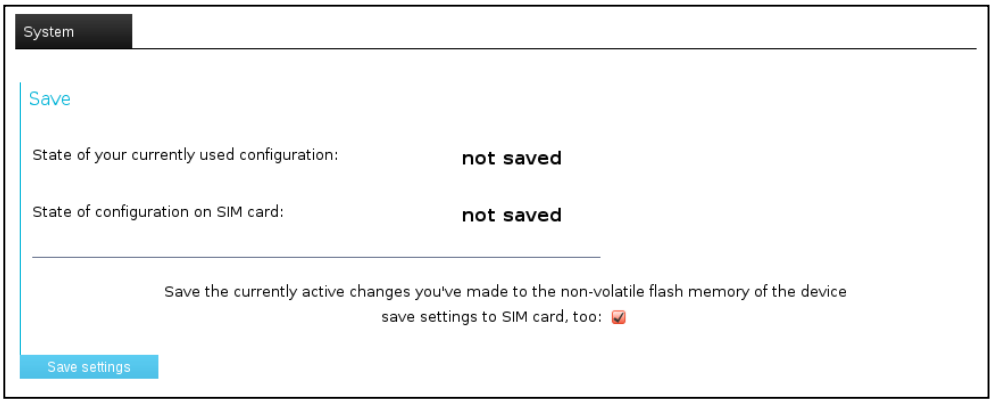
Only SIM cards from ads-tec must be used!

SAVING THE CONFIGURATION ON A SIM CARD

If no SIM card is inserted, the message "No SIM card available" appears.


System
Save
State of your currently used configuration:
saved
State of configuration on SIM card:
no SIM card available
Save the currently active changes you've made to the non-volatile flash memory of the device
save settings to SIM card, too:
Save settings

In order to save the settings to a SIM card, you have to select the "Write settings additionally to SIM card" checkbox in the "Save" dialogue, and to push the Save settings button afterwards.


System
Save
State of your currently used configuration:
not saved
State of configuration on SIM card:
not saved
Save the currently active changes you've made to the non-volatile flash memory of the device
save settings to SIM card, too:
Save settings

REPLACING A DEVICE

Place the SIM card in the switched off device and then turn the device on. Settings will now be loaded during booting. The following messages might appear in the Eventlog:

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

EXAMPLES:

Successful loading of settings:
Nov 1 00:00:05 IF1xxx system: successfully loaded config from SIM card

The successful update of a SIM card was saved to a different firmware than before:
Nov 1 00:00:05 IF1xxx system: successfully updated SIM card config to firmware version: 1.1.1



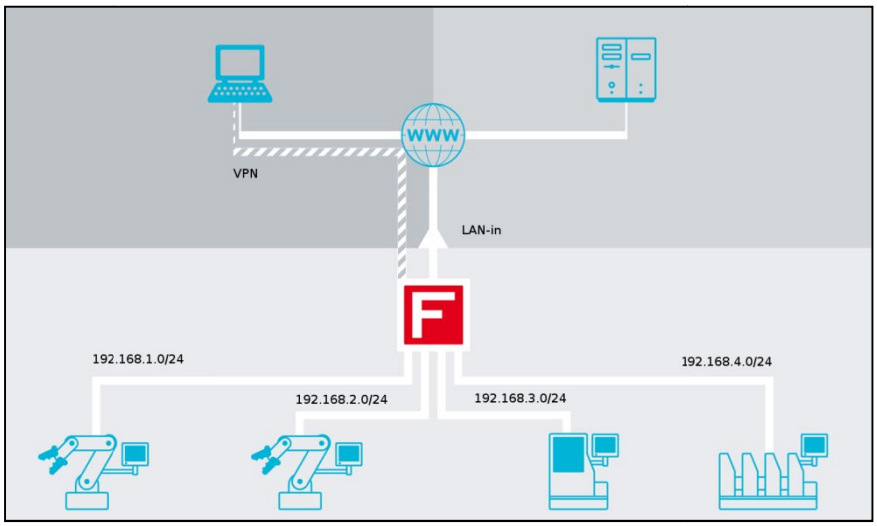
Note:

If a SIM card in a device is loaded with the up-to-date firmware version and the same SIM card put into a device with an older firmware version afterwards, all newly set up parameters of the later firmware version are deleted since they are unavailable in the older firmware version. This also applies to the data stored on the SIM card itself.
(Only applicable for RAP/RAC!) A SIM card including configuration cannot be switched between two different types of devices. If, for example, the configuration of a RAP111x type is stored to a SIM card, this SIM card will not be readable if you put it into a RAC111x type device. But the card can be overwritten at any point in time.
Some RAP/RAC devices with an older hardware version can't manage this function despite having a SIM card slot. SIM card functions will not be visible in these cases.

11.16 EXTENDED IP ROUTER MODE

GENERAL

In regular IP router mode, the IF1000 device connects two different subnets with each other. The LAN-out interface works as a switch with four ports, which means that there is only a single IP address for all the outputs of the LAN-out interface. In the extended IP router mode, on the other hand, each port defines an own subnet including an own IP address. The IF1000 will then, as a result, route between five different subnets.



Note:

In extended mode, the switch cannot be configured as a VLAN switch, and can also not convey any VLAN packets.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

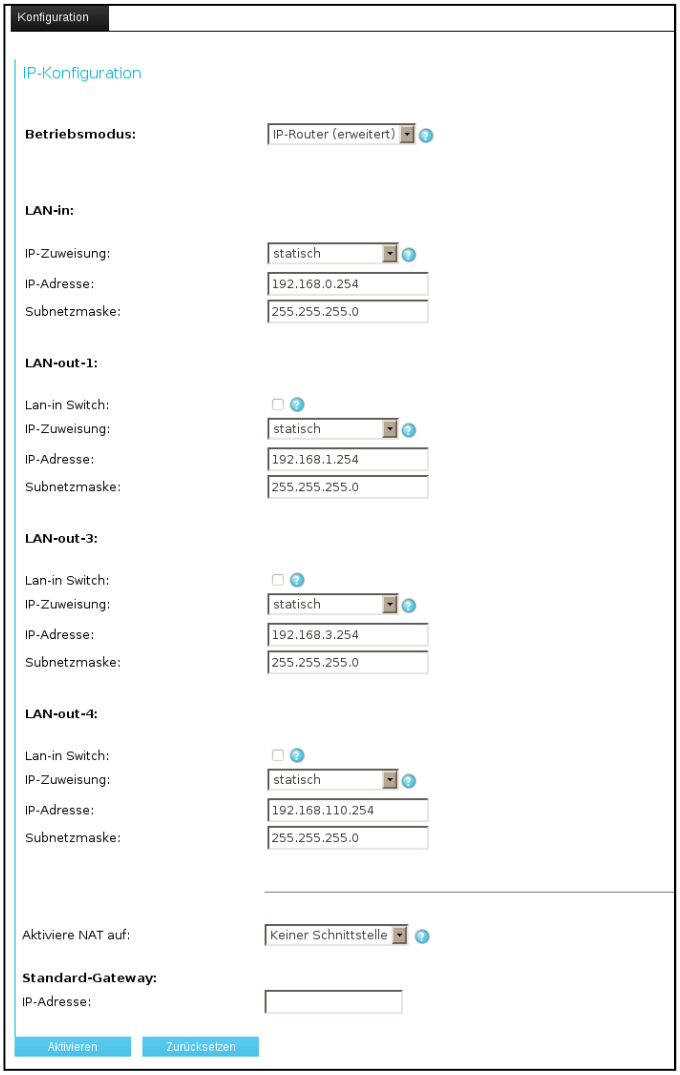
CONFIGURING THE EXTENDED IP ROUTER MODE

Basic configuration

If you select the IP router (extended) mode in the IP configuration, subnets may individually be specified for each port. In this mode, all "LAN-in" interfaces as well as all LAN-out ports are always available for configuration.

Every interface can statically be configured or configured as per DHCP. Additionally, "PPPoe/DHCP" can be configured with any hardware interface which allows a connection with a connected DSL modem to be also established on one of the LAN-out ports.

Depending on the actual OpenVPN configuration, the interfaces "LAN-out (internal)" (with OpenVPN layer 2 connections) or "L3-VPN" (with OpenVPN layer 3 connections) can additionally be available. This requires that first a connection is defined in the "Configuration ☐ VPN ☐ OpenVPN" menu. Subsequently, the corresponding interfaces can be configured on the IP configuration page.



Lan-in switch configuration

Physical interfaces can only be connected with the LAN-in port on an Ethernet level, if the IP router extended mode is used, which means that virtual VPN interfaces are excluded. The principle is similar to the regular IP router mode, where the LAN-out ports are connected with a "LAN-out" interface. But there is an important difference: The LAN-out ports in the IP router mode are connected with each other by using a hardware switch. Packets which for instance arrive at port 1 and are destined for port 2 cannot be filtered by the Industrial Firewall, even not by using the layer 2 packet filter. The Industrial Firewall system doesn't get to know these packets, since they are forwarded by using the integrated hardware switch regardless of the firewall.

But if these interfaces are connected with each other by using the "LAN-in switch" option, the situation is different: The hardware switch no longer independently forwards the packets on an Ethernet level. This is now the responsibility of the Industrial Firewall system - realised by the software. On the one hand, the throughput is slightly lower than the maximum value, as a result. But on the other hand, it is of great benefit that every port of the LAN-in software switches in the layer 2 packet filter can now be used for configuration.

The data traffic between the involved LAN-in switch ports now basically behaves as if the connected devices are all connected with a single switch, which in turn is connected with the LAN-in port of the Industrial Firewall as well. But there are two important differences:

The data traffic between the LAN-in switch ports passes through the Industrial Firewall system and can be restricted by the layer 2 packet filter.

The different possible NAT modes (refer to the "NAT" use case) apply here anyway, i.e. a packet is probably modified by a NAT, by port forwarding or by a 1:1 NAT setting, if required, before it is forwarded on an Ethernet level.

Please select the corresponding checkbox for the LAN-out port in question on the IP configuration page if you want to add LAN-out ports to the LAN switch in IP router extended mode. The corresponding LAN-out port has then no longer an individual IP address. The IP address of "LAN-in" applies to all LAN-in switch ports instead.

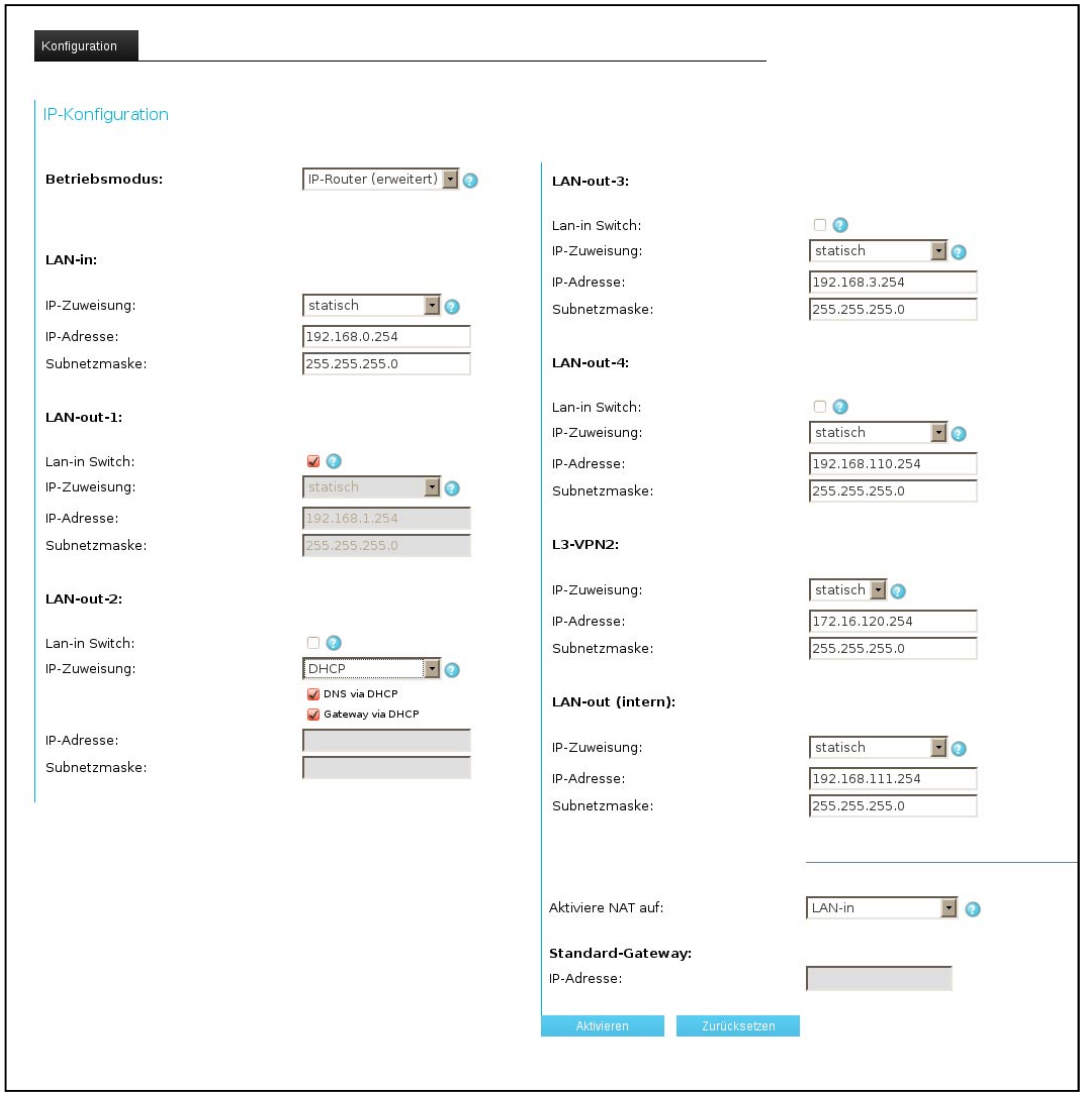
Additional OpenVPN interfaces

Depending on the actual OpenVPN configuration, the interfaces "LAN-out (internal)" (with OpenVPN layer 2 connections) or "L3-VPN" (with OpenVPN layer 3 connections) can additionally be available. This requires that first a connection is defined in the "Configuration ☐ VPN ☐ OpenVPN" menu. Subsequently, the corresponding interfaces can be configured on the IP configuration page.

OpenVPN layer 2 connections (of which a maximum of 10 is possible) are all together connected with the "LAN-out (internal)" interface on an Ethernet level. As a result, the tunnels are all available within a single subnet. The devices at the tunnelling endpoints can communicate with each other via the tunnel by using any type of layer 3 protocol, e.g. IPv6.

OpenVPN layer 3 connections have an individual IPv4 interface. They have therefore their own subnet and can only directly communicate by using IPv4 packets. This means in particular that the endpoints of corresponding routes must be configured for the foreign subnet, as a result. Then you have to configure an IP address and subnet mask for every tunnel on the Industrial Firewall.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen


Konfiguration
IP-Konfiguration
Betriebsmodus:
IP-Router (erweitert)
LAN-in:
IP-Zuweisung:
statisch
IP-Adresse:
192.168.0.254
Subnetzmaske:
255.255.255.0
LAN-out-1:
Lan-in Switch:
IP-Zuweisung:
statisch
IP-Adresse:
192.168.1.254
Subnetzmaske:
255.255.255.0
LAN-out-2:
Lan-in Switch:
IP-Zuweisung:
DHCP
DNS via DHCP
Gateway via DHCP
IP-Adresse:
Subnetzmaske:
LAN-out-3:
Lan-in Switch:
IP-Zuweisung:
statisch
IP-Adresse:
192.168.3.254
Subnetzmaske:
255.255.255.0
LAN-out-4:
Lan-in Switch:
IP-Zuweisung:
statisch
IP-Adresse:
192.168.110.254
Subnetzmaske:
255.255.255.0
L3-VPN2:
IP-Zuweisung:
statisch
IP-Adresse:
172.16.120.254
Subnetzmaske:
255.255.255.0
LAN-out (intern):
IP-Zuweisung:
statisch
IP-Adresse:
192.168.111.254
Subnetzmaske:
255.255.255.0
Aktiviere NAT auf:
LAN-in
Standard-Gateway:
IP-Adresse:
Aktivieren
Zurücksetzen

11.17 REMOTE CAPTURE

GENERAL

"Remote capture" is used for recording and analysing the traffic of any active firewall interface via the network from a Windows PC, on which Wireshark is installed (http://www.wireshark.org).

Note:

This feature is designed for debugging. The capture server should only be used for short periods of time and if required, in order to minimise the security risk since authentication is impossible.

FIREWALL CONFIGURATION

The remote capture service can be enabled in the Diagnostics/Remote capture menu and then listens to the default port 2002 for any inbound connections. The IP address of the computer which is supposed to make the recording, must explicitly be specified (e.g. 192.168.253.168) in order to minimise the security risk since no authentication is possible:



As an additional security feature, only a single connection is permitted at any point in time, i.e. the specified computer cannot make two recordings simultaneously.

LAN-out regularly works as a switch. That means if two devices communicate with each other (e.g. on port 1 and port 2), the packets are forwarded within the switch by the hardware, so that they do not reach the firewall system, and cannot be recorded, as a result. The "Enable hub mode on LAN-out" option can be used for making the entire traffic between the ports visible, if required. All packets are forwarded to all ports including the firewall system in hub mode.

Usually only access right violations are logged (if an attempt is made to either establish the connection from a wrong IP address or to establish two connections at the same time). With "Message details", information about the connection (control/data channel) and the overlistened interfaces is also recorded.

Note:

A warning is output in the Eventlog every hour in order to avoid that this service might keep running unintentionally.
The remote capture connection between the firewall and the recording computer is

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

always filtered in order to ensure a reasonable recording.
The hub mode takes about 10 seconds until it is activated. That means if the remote capture is started too early, the first packets might not be captured in the log.

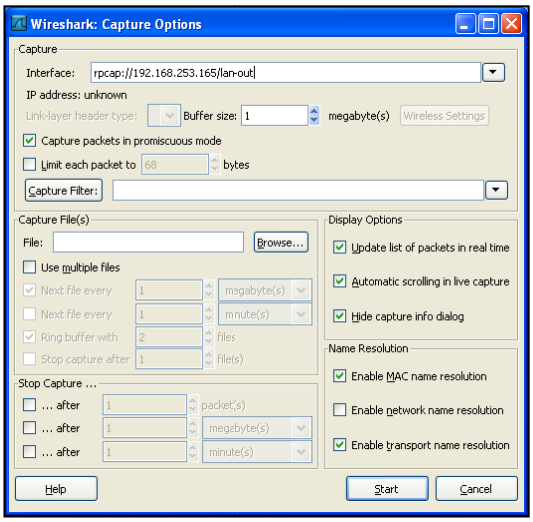
WIRESHARK CONFIGURATION UNDER WINDOWS XP

The minimum requirement is that Wireshark version 1.0.6 and WinPcap version 4.0.2 or any later version is used. In all earlier versions it was impossible to stop and then restart the capture process.

The remote interfaces must explicitly be specified in the "Show the capture options" option (the second icon in the main toolbar) or in the "Capture/Options" menu item:


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Help
Show the capture options...
Filter:
Expression... Clear Apply

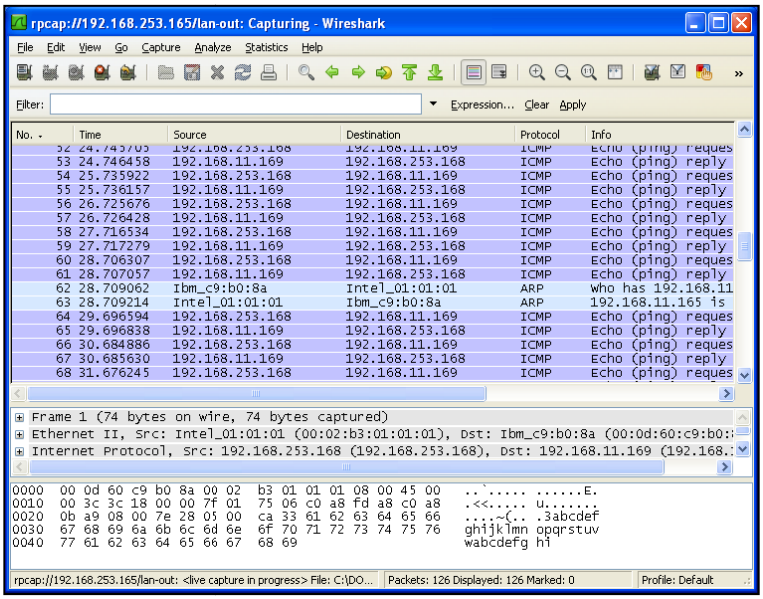
"rpcap://192.168.253.165/LAN-out" is for instance the remote capture URL for recording the data traffic on "LAN-out" of the firewall with IP address 192.168.253.165:



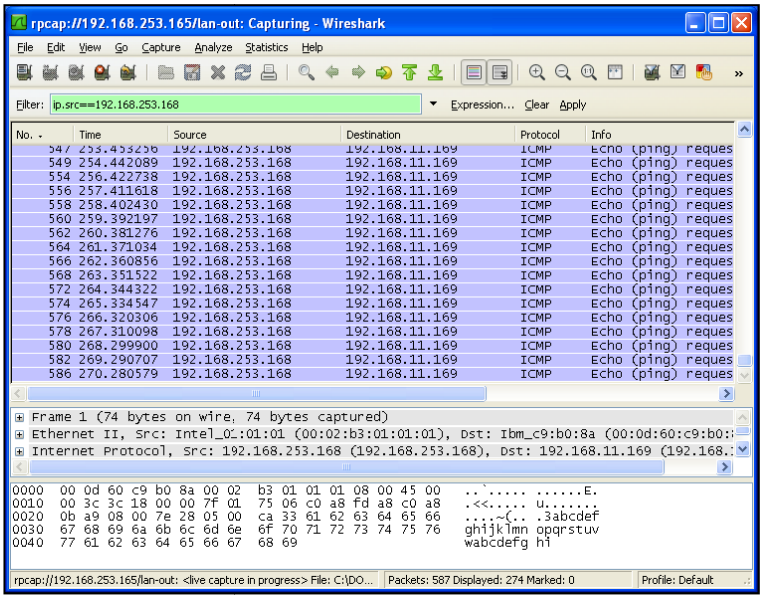
The "rpcap://..." prefix must always be specified and identifies the capture per network. The firewall interface designations can be written regardless whether upper or lower case is used and should match the names used in the web interface. The IPsec interfaces are exceptions - the space in front of the (IPsec) must be omitted there - and the PPPoE interface, which can be addressed with either "dsl" or "pppoe". Here is an example of the detailed designations:

Interface	Remark
DSL PPPoE	PPPoE uplink (independent on the interface it is based on, and via which the connection was established)
LAN-in	Always exists
LAN-out	Always exists
LAN-out-x	The individual ports (x in the name is always to be replaced with 1, 2, 3 or 4) only exist in extended IP router mode. LAN-out is then the internal endpoint for the layer 2 OpenVPN connections.
SERVICE	Exists if a modem connection is present
L2-VPNx	The individual OpenVPN interfaces (x in the name is to be replaced with 1 to 10) always exist with Server connections, but with client connections they exist only if the client connection is actually established.
LAN-in(IPsec) LAN(IPsec) LAN-out-1(IPsec) LAN-out-2(IPsec) LAN-out-3(IPsec) LAN-out-4(IPsec) SERVICE(IPsec)	According to the IPsec configuration, there is a dedicated IPsec interface (e.g. LAN-in(IPsec) as a tunnel endpoint, on which the traffic is visible without encryption. Only the encrypted packets are visible on the interface which forms the basis (e.g. LAN-in). LAN(IPsec) belongs to the tunnel endpoint for LAN-out.

If the connection was established successfully, the packets can be viewed and filtered just like in a regular case by using Wireshark:



© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen





Note:

Should the Windows firewall be enabled, enabling only port 2002 is not enough, because a separate data connection is used, where any port number is possible, and which is similar to FTP. The ads-tec Industrial Firewall, on which the remote capture server runs, does not require any particular filter settings.

WIRESHARK ERROR MESSAGES

Wireshark shows a window with the error message "The capture session could not be initiated" and with a detailed cause in parentheses if establishing the connection fails. The most frequently occurring causes are explained below.

ioctl: No such device

The specified interface does not exist. Either something is wrong with the notation (refer to above table), the firewall is differently configured, or the interface is temporarily unavailable (the PPPoE interface e.g. only exists with an existing uplink).

Is the server properly installed on <IPADDRESS>? connect() failed: ...

The specified IP address <IPADDRESS> is unavailable or the remote capture service does not run on this location.

The host is not in the allowed host list. Connection refused.

The IP address of the own computer does not match the address allowed in the firewall web interface (this causes an entry in the Eventlog of the firewall).

Too many clients

A connection with the remote capture server already exists. It was either established by another Wireshark application or by another network subscriber with an identical IP address by accident (causes an entry in the Eventlog of the firewall).

11.18 1:1 NAT NETWORK MAPPING

GENERAL

This document shows how the extensive NAT functions of the ads-tec Industrial Firewalls can be used in practice.
NAT (network address translation) is the designation of the process, in which the IP address of an IP packet is replaced by another address. There are several options for this translation:

"NAT / 1:1 NAT / Masquerading": The IP address of a certain range is replaced by a single IP address under certain conditions. Such a condition could be, for instance, if the packet is sent via an interface, on which masquerading is enabled.
"Port forwarding / PAT (port address translation)": A target address is substituted in this case, where the port number of the transport protocol (either UDP or TCP) is translated accordingly. This option is mostly used for enabling the establishment of connections with hosts, which would be unavailable due their NAT routers otherwise.
"1:1 NAT / symmetric NAT": An entire address range is used for the substitution in this case, which results in the fact that the sender or target is not unambiguously identified. Establishing the connection is then possible from both sides of the NAT.

NAT (MASQUERADING)

The configuration is made in the "Configuration → IP configuration" menu. Depending on a certain network interface, all packets sent by using this interface are translated. Each packet is provided with the IP address of the firewall on this interface as the sender IP.

PORT FORWARDING

The settings are made in the "Configuration → Network → Port forwarding" menu. You'll find more information about port forwarding in the "Port forwarding" use case specifically created for this topic.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

1:1 NAT NETWORK MAPPING

FUNCTIONALITY

Usually it is impossible to create a router in such a way that the same IP address range (e.g. 192.168.0.0/24) can be used on different network interfaces at the same time. A switch is usually used for this function, but routing is then impossible.

It can happen that devices which have the same IP address are supposed to communicate with each other. Normally, the configuration should be arranged between different devices so that all devices have an unambiguous IP address. But in some cases, this is possible only with a huge effort, or this address conflict can only be resolved by using NAT routers.
Our ads-tec Industrial Firewalls are using an exclusive NAT technology to bypass this issue - the network mapping technology - which saves the additional introduction of routers. Every one of these "identical" subnets would have to be masked with an individual NAT router, if the commonly available methods would be used.

Identical subnets can be defined for different routing interfaces (refer to figure 1) in the "Configuration → Network → 1:1 NAT" menu. This even allows that devices with the same IP address can communicate with each other. A second IP address range, the so-called "Public subnet", is used for each interface in order to allow this. If two devices are connected with different interfaces, which have the same IP address (e.g. 192.168.0.1), it looks for every host like the communication takes place with a device from the corresponding other public subnet.
Regardless whether identical subnets are masked in this way or not, this functionality can also be used for a regular symmetric 1:1 NAT, of course.



Note:

The designations "private Subnet" and "public Subnet" in the 1:1-NAT terminology have nothing to do with the three private address ranges of 10.0.0.0/8, 172.16.0.0/12 and 192.168.0.0/16 as they have been defined in the RFC 1918 standard.
"Private" and "Public" in this case means that the corresponding "Internal" and "External" subnets have different appearances. The private IP range is isolated on the corresponding interface, so that the IP addresses of the "public" range even have to be used for the filter rules and routing entries in the firewall. This means that in a sense the private addresses are "unknown" even for the firewall - except for the settings on the 1:1 NAT page, of course.

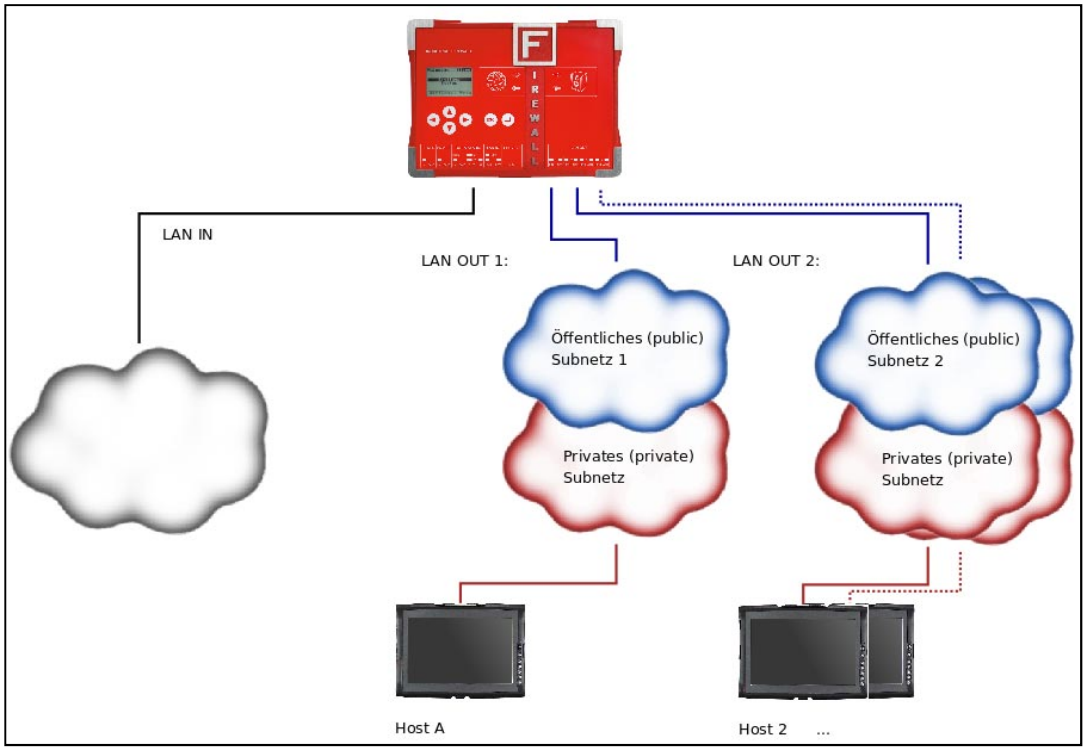
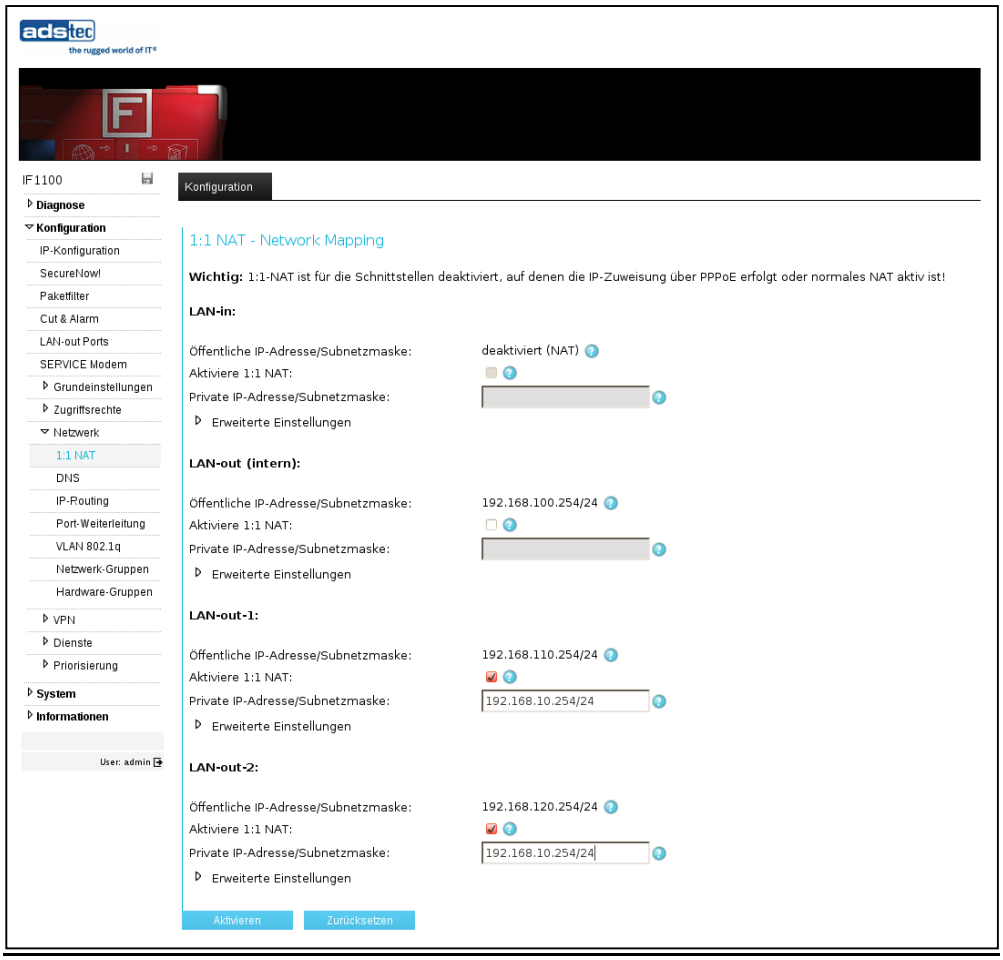


Figure 1: 1:1 NAT with (identical) private subnets



© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

ASSIGNMENT OF PRIVATE TO PUBLIC ADDRESSES

The public IP address results (1:1) from the private IP address of a certain device by combining a prefix from the subnet designation (length in accordance with the subnet mask) with a suffix from the device address.

EXAMPLE:

The device has the IP address 172.16.100.40 in the private subnet 172.16.100.20/24. The public subnet is 10.20.30.0/24. The prefix of the public IP address of this device is 10.20.30 (the first 24 bits are fixed, i.e. there are 3 tuples with 8 bit each). The suffix is taken from the remaining bits of the device address, i.e. "40" in this case. According to this procedure, the device is mapped to the public IP address "10.20.30.40".

COMPLEX EXAMPLE:

Let's assume that the device from the previous example again has the IP address 172.16.100.40, but the size of the subnet is "/28" this time. This means that it contains the IP addresses 172.16.100.32 – 172.16.100.47, since the first 28 bits (172.16.100.32) are fixed, and only the last 4 bits are variable. The device now has the ninth IP address in this subnet, and this is 1:1 mapped to the public range. This means in particular, that the device also has the ninth IP address there (Attention: zero is counted as well).
Let's assume that the public subnet is defined as 10.20.30.0/28 this time. If you combine this with the last 4 bits of the private IP address of this device, you'll obtain the public IP address of the device. It is „10.20.30.8".



Note:

Together with the "private subnet" setting on the configuration page for 1:1 NAT, the IP address of the firewall in the private range is defined, at the same time (refer to figure 2). The Industrial Firewall has two IP addresses in this case: one is the private IP address for devices connected with the corresponding 1:1 NAT interface, and the other one is the public IP address for the rest of the world. Here, you should ensure that the 1:1 allocation between the private and public IP address is preserved, since it is defined by the user. So if the firewall has for instance the public IP address "192.168.0.99/24" (this is the 100th address in the subnet), you'll have to ensure that the 100th address of the private subnet is also used for "private subnet") (e.g. "192.168.1.99/24"). If this is impossible for any reason, e.g. if the firewall is assigned with "192.168.1.100" as the private address, then you'll have to expect trouble for an existing device in the private network, which uses the address "192.168.1.99". This address should then not be used for it.

COMMUNICATION VIA 1:1 NAT / NETWORK MAPPING

For communication beyond the 1:1 NAT borderlines, you'll have to ensure that the devices behind the 1:1 NAT, i.e. in the private subnet, are always addressed with their public IP address. Moreover, the addresses of private subnets must never be referenced in a different place on the Industrial Firewall, e.g. where routing entries or filter rules are concerned. The public IP addresses must be used in these places.

EXAMPLE:

The network topology as shown in figure 3 should be provided. LAN-out-1 and LAN-out-2 are configured with 1:1-NAT / Network mapping and use identical private networks (192.168.10.254/24).
The firewall itself can be reached in the 192.168.10.0/24 network by using LAN-out-1 or LAN-out-2 with the IP address 192.168.10.254.

One device each with IP address 192.168.10.1 is available at the LAN-out-1 and LAN-out-2 interface. If you wish to communicate with one of these devices via the firewall, you'll have to use the public IP address of the corresponding device. This is 192.168.110.1 with host A and 192.168.120.1 with host B.
This also applies to the communication between the two hosts: If e.g. host A tries to establish a connection with host B, host A must use 192.168.120.1 as the destination address. In the other direction, host B "knows" host A only as "192.168.110.1".

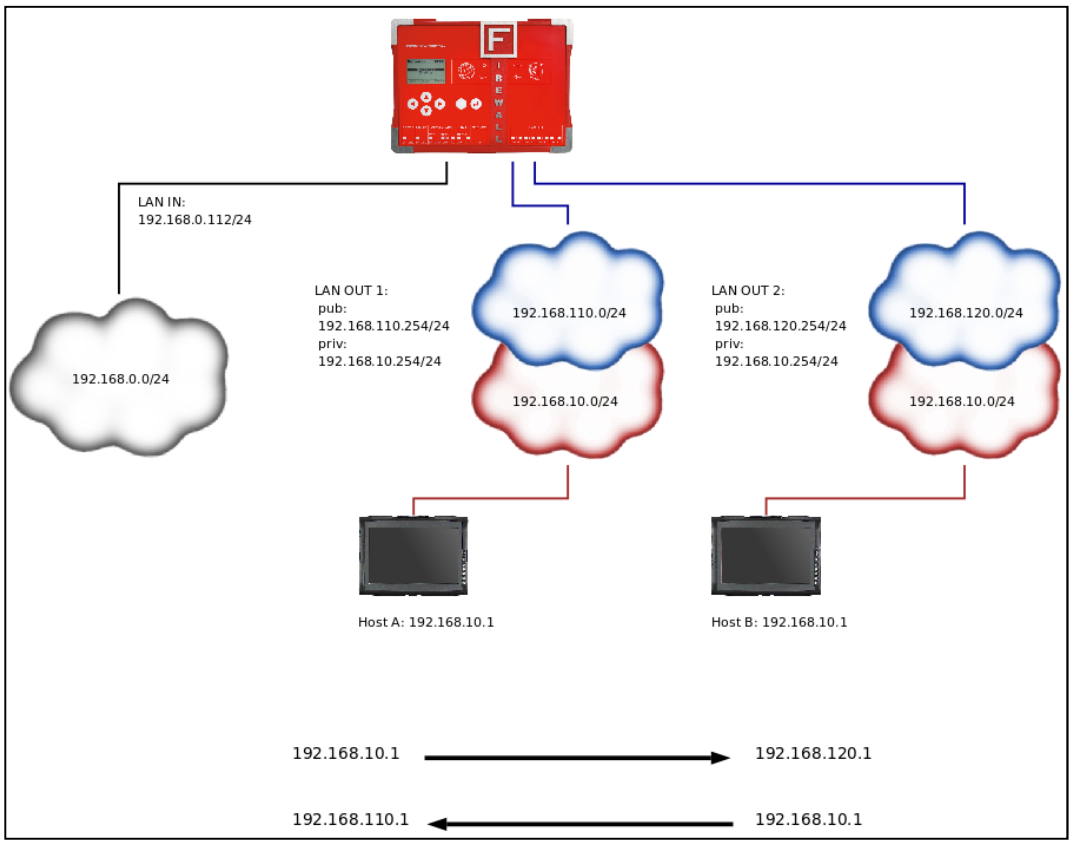


Figure 2: Network mapping network topology, simple case

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

1:1 NAT - ADVANCED SETTINGS

The IP address range which is used as a private subnet with 1:1 NAT is also used by hosts on other public interfaces, under certain circumstances. If, for example, a scenario according to figure 4 is present, then the address range "192.168.10.0/24" is used by host C, which is located on the LAN-in side of the firewall. In a simpler case, it would be sufficient to make a 1:1 NAT configuration for LAN-in as well, but this cannot be done in our example for two reasons:

→NAT (masquerading) is enabled on LAN-in, and 1:1 NAT cannot additionally be used, as a result.

→The subnet connected with LAN-in is the "192.168.0.0/24" subnet. The packets from host C with the "192.168.10.0/24" address range are forwarded to the firewall by an additional router. But 1:1 NAT can only be defined for the next directly adjacent subnet, since the firewall on the corresponding interface is also assigned with an IP address from this subnet.

The "Advanced settings" including "Double sided network mapping" are provided in order to solve the arisen address conflict in spite of these facts. Here another network range is defined, which is used by host C in certain situations (and by all other hosts from this range), i.e. an additional, specific 1:1 NAT is enabled, which is applied independently on the interface of the sender.

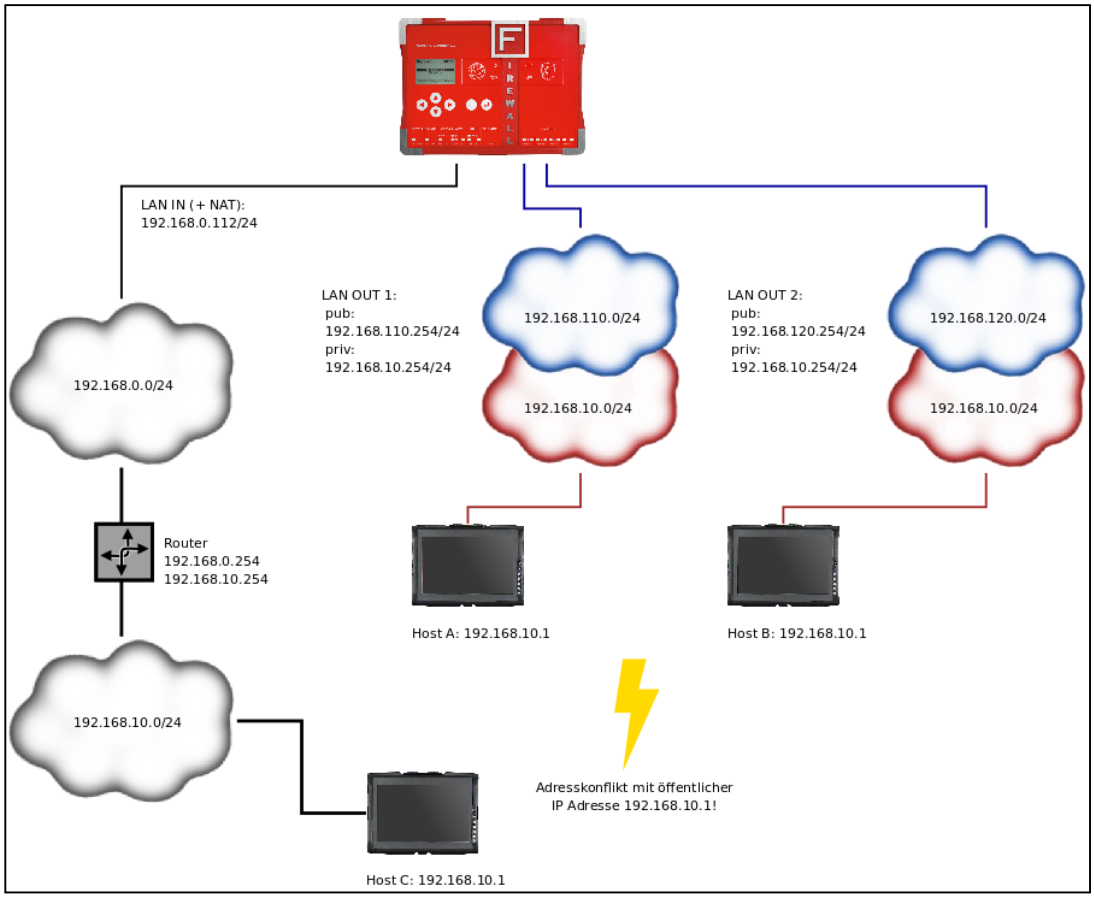


Figure 3: Network mapping network topology, complex case

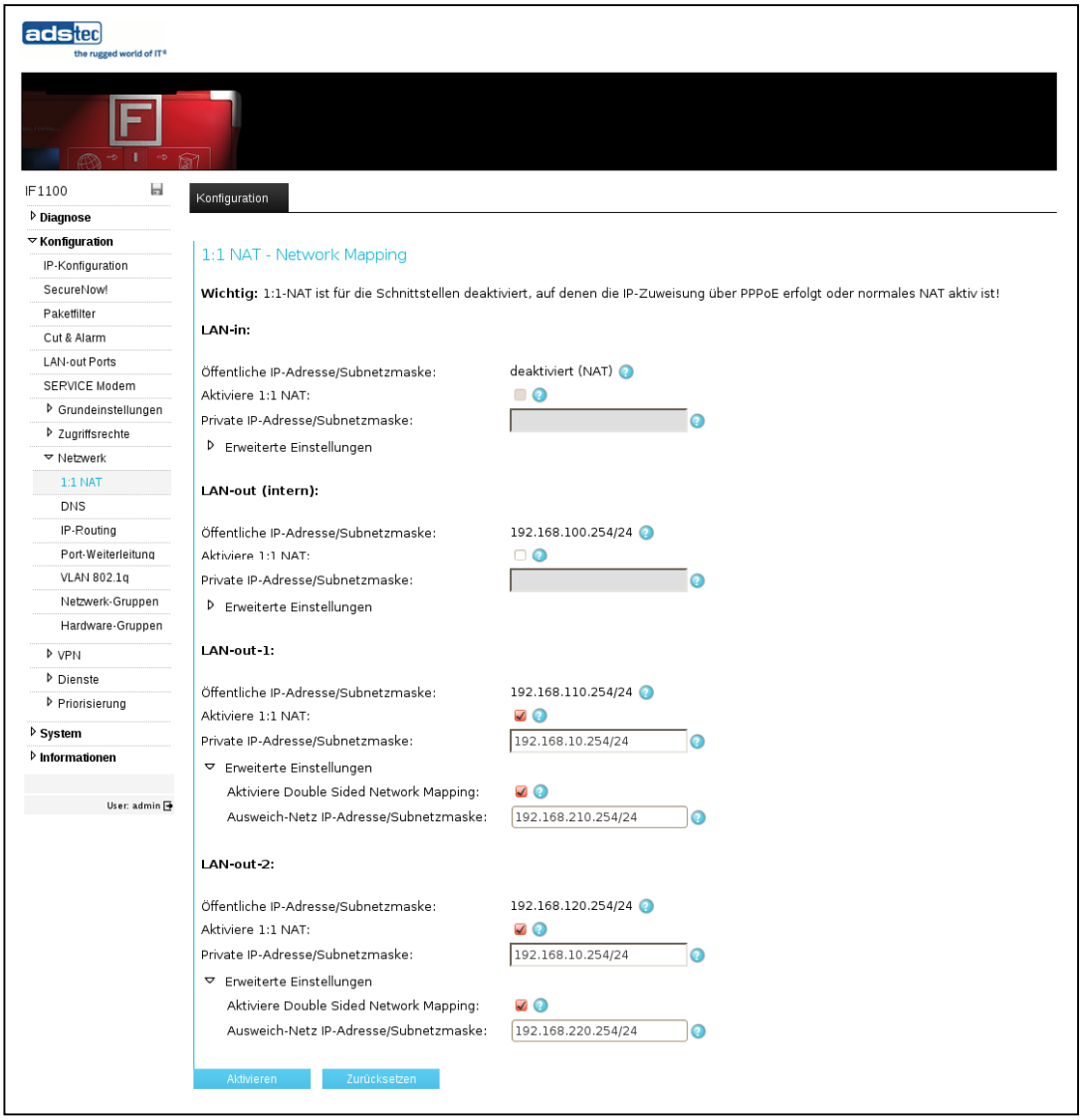
EXAMPLE:

The same settings like in the previous examples, as well as the settings and assumptions from figure 5 and figure 4, shall apply.

Furthermore, there are two avoidance address ranges configured for "Double sided network mapping": 192.168.210.0/24 for the private subnet of LAN-out, port 1, and 192.168.220.0/24 for the private subnet of LAN-out, port 2.

So there are now three hosts in total with the same IP address "192.168.10.1": host A, host B and host C. The IP address of host C is public in contrast to host A and B. As a result, it can happen that packets from host C with this public IP pass through the firewall (as explained before). By using the settings from figure 5, the communication between host A and host C is processed as follows:

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen



TCP PORT 80 VIA LAN-IN NAT + PORT FORWARDING:

→A port forwarding entry exists on the firewall, as a result of which TCP packets for IP address "192.168.0.112" and port "2000" are forwarded to host A, i.e. to "192.168.110.1" and port 80.

→NAT (masquerading) is enabled on LAN-in.

→Host C reaches host A via IP 192.168.0.112 and port 2000. At host A, host C appears under the masked source address 192.168.210.1

→Host A reaches host C by using IP 192.168.210.1.



Note:

The previous example with port forwarding would also work if you do it in the following way: Forward all protocols and ports to the IP "192.168.110.1", except for TCP port 80 (in order to retain continued access to the firewall web interface).

A port forwarding entry, which forwards all TCP packets with destination IP "192.168.210.1" and port "80" to the IP "192.168.0.112" and port "80", must be defined first.

Then an entry is added, which forwards all packets of all protocol types with destination IP "192.168.0.112" to the IP "192.168.110.1". The order is critical here: The first entry always has priority over the second, and in this way, the desired effect is achieved.

VIA LAN-IN WITH ROUTING:

- On host C, there is a route of the form "default via 192.168.10.254" (IP of the router between the grey clouds in figure 4) or a more specific one.
- On the router, there is a route of the form "default via 192.168.0.112" or more specific.
- On the Industrial Firewall, there is a route of the form "default via 192.168.0.254" or more specific.
- On host A, a route of the form "default via 192.168.10.254" exists (this was always tacitly implied in the previous examples).
- Host C reaches host A by using IP 192.168.110.1.
- Host A reaches host C by using IP 192.168.210.1.
- Host B reaches host C by using IP 192.168.220.1.
- The firewall itself or hosts on other, probably defined interfaces (LAN-out (internal), LAN-out port 3, etc.), reach host C by using the IP 192.168.10.1.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

11.19 PRIORITISATION / SHAPING

GENERAL

In general, there are two different ways by which you can ensure that a sufficient bit rate is available for a certain Ethernet based form of communication:

1) Shaping.
   Different traffic classes defined by certain protocol values are assigned with fixed bit rates. Disadvantage: A traffic class is already restricted when reaching the defined limit, even if the maximum possible overall bit rate is not yet fully utilised.

2) Prioritisation.
   Only once the overall bit rate reaches the maximum possible overall bit rate, certain traffic classes are prioritised over others. Disadvantage: In the worst case scenario, a traffic class with the highest priority could suppress any other traffic altogether.

The IF1000 series devices can manage the following modes:

Pure prioritisation:

No type of traffic is restricted in a regular case. Only if the interface traffic limit is reached, which means that the related interface has reached maximum utilisation, certain types of packets are preferred to others.

Pure shaping:

For certain traffic types, only a fixed bit rate limit is available. This limit is never exceeded, even if other classes do not utilise their limit and if the interface bit rate limit is not fully utilised.

Prioritisation + shaping:

This is a mixed form of both, the "pure prioritisation" and the "pure shaping" mode. The following trend applies: Until reaching the maximum bit rate, the function is similar to "prioritisation", but beyond that, the "pure shaping" functionality is applied. The general disadvantages of pure shaping and pure prioritisation are avoided by this combination.

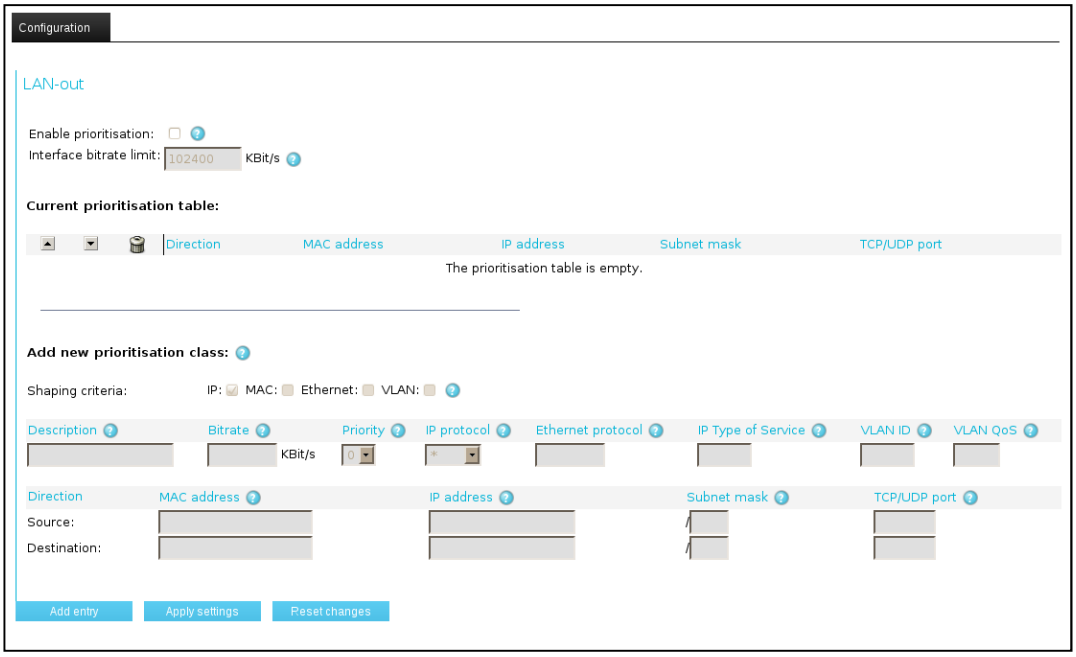
But with all applications, the interface limit has to be observed, even if the physical prerequisites would allow higher speeds.

Exception: If the total of all guaranteed bit rates of the individual traffic classes exceeds the specified interface limit, then the interface limit is exceeded, provided that all traffic classes utilise their assigned limits.



Note:

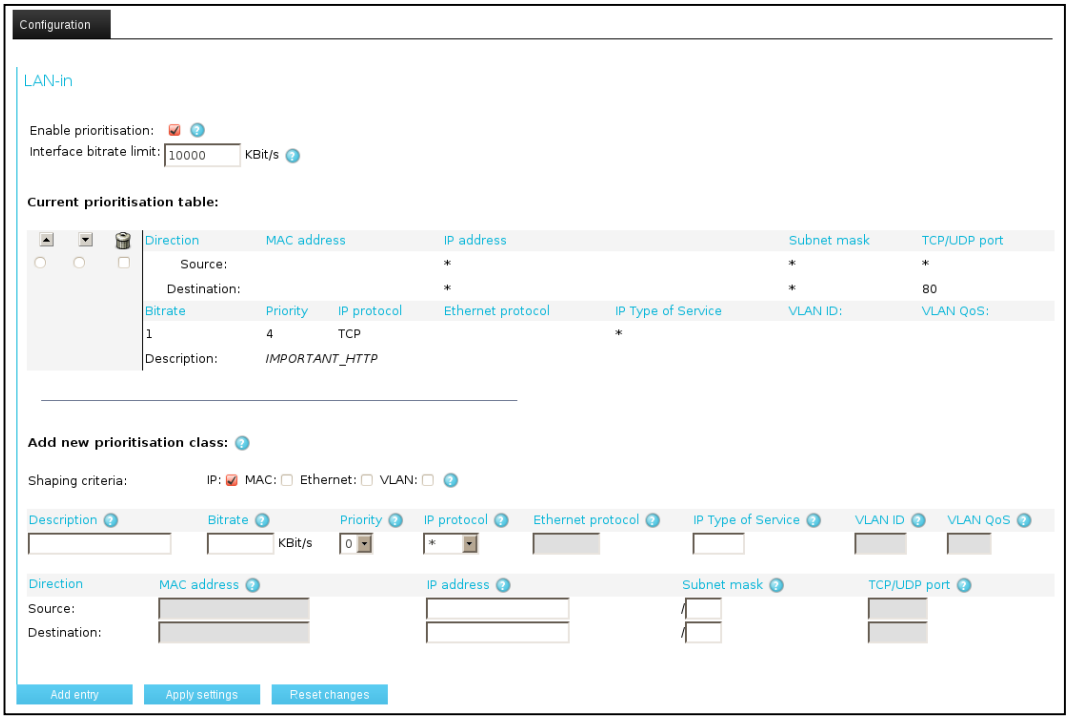
*It is always only the **outbound** data traffic, which can be prioritised or restricted for every physical interface. The inbound traffic can only be prioritised or restricted by being treated at the corresponding outbound interface and when exiting the device.*



PURE PRIORITISATION

CONFIGURATION EXAMPLE:

The interface limit is set e.g. to 10.000 kbit/s, and exactly one prioritisation class is defined, which has a bit rate of 1kbit/s and a priority of < 7.



© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

EFFECTS:

There is no effect as long as the maximum bandwidth, i.e. the 10,000 kbit traffic speed, is not reached.

Moreover: The prioritised class is preferred. It gets as much bandwidth as it needs until the full limit of 10,000 kbit is reached. If it doesn't need the full bandwidth, then the remaining traffic gets the rest of it.

PRIORITISATION + SHAPING

Shaping means that the affected traffic class is artificially restricted in its bandwidth.

Configuration example:

An interface limit is set, for example at 10,000 kbit/s.

Different classes are created, which have different bit rates and different priorities.

→Class 1: 5,000 kbit; priority 5

→Class 2: 3,000 kbit; priority 1

→Class 3: 2,000 kbit; priority 2


Configuration
LAN-in
Enable prioritisation:
Interface bitrate limit: 10000 KBit/s
Current prioritisation table:
Direction MAC address IP address Subnet mask TCP/UDP port
Source: * * *
Destination: * * 80
Bitrate Priority IP protocol Ethernet protocol IP Type of Service VLAN ID: VLAN QoS:
5000 5 TCP *
Description: HTTP_MAX_PRIO
Direction MAC address IP address Subnet mask TCP/UDP port
Source: * * *
Destination: * * *
Bitrate Priority IP protocol Ethernet protocol IP Type of Service VLAN ID: VLAN QoS:
3000 1 UDP *
Description: UDP_MIN_PRIO
Direction MAC address IP address Subnet mask TCP/UDP port
Source: * *
Destination: * *
Bitrate Priority IP protocol Ethernet protocol IP Type of Service VLAN ID: VLAN QoS:
2000 2 ICMP *
Description: ICMP_CLASS

WARNING:

Traffic which does not belong to any of the created prioritisation classes is treated like a class with a guaranteed bit rate of 1kbit and priority 7. This behaviour can be modified if a class with the desired properties is created, for which no header properties are specified.

Note:

The total of all bit rates of all individual prioritisation classes, which is in this example 5,000+3,000+2,000=10,000, must never exceed the interface limit in this mode.

EFFECTS:

Even before the overall traffic reaches the maximum bandwidth:

No prioritisation class obtains more than 120% [1] of the guaranteed bandwidth. If there is, for example, only traffic of class 1 and no other traffic, the available bandwidth is only utilised with 60,000kbit.

If the overall traffic reaches the maximum bandwidth, but there are classes which don't utilise their individually guaranteed bandwidth:

Every prioritisation class is only assigned with an additional bandwidth proportion if there is no class with a higher priority, which also claims more bandwidth. Even then, the maximum additional bandwidth is limited to 20% [1].

If the overall traffic reaches the maximum bandwidth, but all classes utilise their individually guaranteed bandwidth:

In this example, the overall available bandwidth would just precisely be utilised, and all classes would exactly receive their guaranteed bit rate and nothing more.

[1]: Applies if the total of all class bit rates equals the interface limit. If the total is smaller, the percentage is increased accordingly.

PURE SHAPING

Pure shaping means that the specified priorities lose their significance. Every class gets exactly the guaranteed bit rate but nothing more.

CONFIGURATION EXAMPLE:

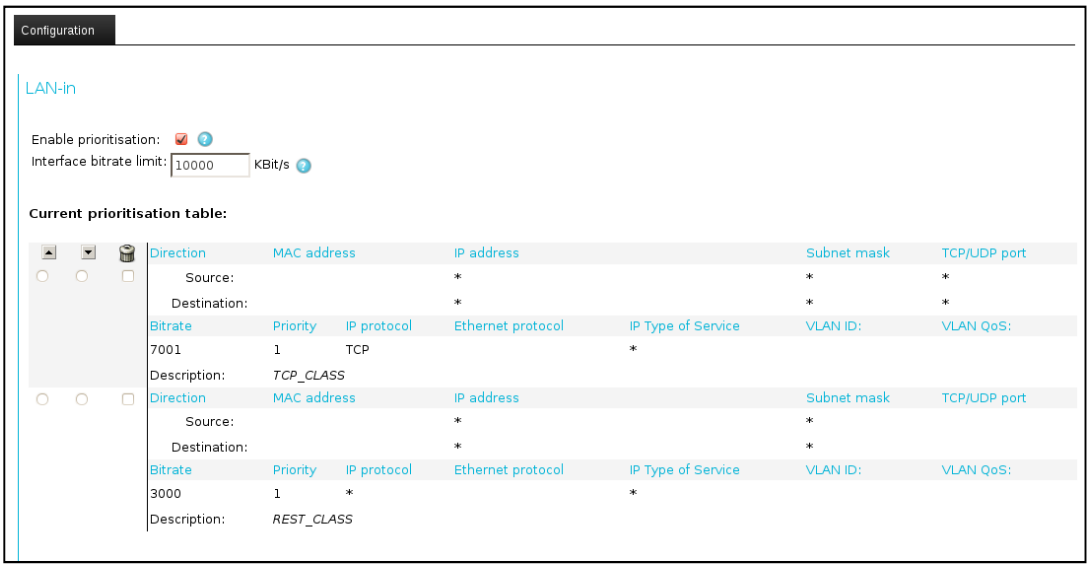
An interface limit is set, for example at 10,000 kbit/s.

Different classes with different bit rates are created.

The total of all bit rates is slightly higher than the interface limit, e.g.

→Class 1: 7,001 kbit/s

→Class 2: 3,000 kbit/s


Configuration
LAN-in
Enable prioritisation:
Interface bitrate limit: 10000 KBit/s
Current prioritisation table:
Direction MAC address IP address Subnet mask TCP/UDP port
Source: * * *
Destination: * * *
Bitrate Priority IP protocol Ethernet protocol IP Type of Service VLAN ID: VLAN QoS:
7001 1 TCP *
Description: TCP_CLASS
Direction MAC address IP address Subnet mask TCP/UDP port
Source: * *
Destination: * *
Bitrate Priority IP protocol Ethernet protocol IP Type of Service VLAN ID: VLAN QoS:
3000 1 * *
Description: REST_CLASS

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

EFFECTS:

Even before the overall traffic reaches the maximum bandwidth:

→No class receives more than the guaranteed bandwidth. If there is e.g. only traffic of class 1 and no other traffic, the available bandwidth is only utilised with 7,001 kbit/s.

→Traffic which is not covered by any of the classes, always receives the bandwidth, which is available until reaching the maximum bandwidth, as long as none of the classes claims this portion.

If the overall traffic reaches the maximum bandwidth:

→Every class gets exactly the guaranteed bandwidth.

Traffic which is not covered by any of these classes gets 1 kbit/s.

APPLICATION EXAMPLES

EXAMPLE 1:

An important web server in the LAN-out network should always get as much bandwidth as it needs. It is connected with the Internet via LAN-in of the firewall. Only if resources are available in excess of the web server demand should they be usable by other services. This application case corresponds with the "prioritisation" option.

An interface limit is defined at e.g. 100,000 kbit/s for both, LAN-in as well as LAN-out.

A class for TCP destination port 80 including priority 0 and a guaranteed bit rate of 1 kbit/s is created for LAN-out. As a result, the HTTP traffic from LAN-in to the server is prioritised.

A class for TCP source port 80 including priority 0 and a guaranteed bit rate of 1 kbit/s is created for LAN-in. As a result, the HTTP traffic of the return direction is prioritised.

EXAMPLE 2:

A less important web server should always be provided with a guaranteed bandwidth on the uplink interface. It has to share the uplink with the SSH server, which should get a higher priority. Only if the SSH server does not fully utilise its capacity should it be available for the web server up to a certain proportion. This application corresponds with the "prioritisation + shaping" option.

Since the uplink is the connection "bottleneck" in this case, it is sufficient to only create interface classes for this connection type.

For the uplink interface, an interface limit of e.g. 10,000 kbit/s is specified.

A class for TCP source port 80 with priority 3 and a guaranteed bit rate of 7,000 kbit is created for the web server.

A class for TCP source port 22 with priority 1 and a guaranteed bit rate of 3,000 kbit is created for the SSH server.

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

12 Declaration of CE-Conformity

IF1100

Declaration of Conformity / Manufacturer Statement

●PRODUCT

NAME: Industrial Firewall
DESCRIPTION: Firewall
MODEL: DVG-IF1100-001-BU

● MANUFACTURER

ads-tec GmbH
Raiffeisenstr. 14
70771 Leinfelden-Echterdingen
Germany

Tel.: +49 / 711 / 458940
Fax: +49 / 711 / 45894994

● LAWS

EU Council Directive of 3 May 1989 on the approximation of the laws of the Member States relating to Electromagnetic Compatibility (EMC_Directive)

EU-Directive: 89/336/EWG from 5/3/1989 (ABl.EU L No. 139/19)
91/263/EWG from 4/29/1991 (ABl.EU L No. 128/1)
92/31/EWG from 4/28/1992 (ABl.EU L No. 126/11)
93/68/EWG from 7/22/1993 (ABl.EU L No. 220/1)

Adopted in Germany by: EMVG from 9/18/1998 (BGBl I 1998, 2882)

COUNCIL DIRECTIVE of 19 February 1973 on the harmonization of the laws of Member States relating to electrical equipment designed for use within certain voltage limits (LVD-Directive)

EU-Directive: (LVD) 2006/95/EC from 12/27/2006 (OJEU, L 374, page 10-19)
93/68/EWG from 7/22/1993 (ABl.EG L Nr. 220/1)

Adopted in Germany by: 1. GPSGV from 7/11/1979 (BGBl I 1979, 629)

● HARMONISED STANDARDS FOR TESTING

EMC-Directive

a) Electromagnetic emissions
EN 61000-6-4:2001

b) Electromagnetic Immunity
EN 61000-6-2:2005

LVD-Directive

Safety of information technology equipment
EN 60950-1:2001

● STATEMENT

The manufacturer hereby declares product conformity with the fundamental requirements given by the above-described directives of the European Union. The tests applicable according to the harmonized standards mentioned above have been fulfilled.
The CE labeling was assigned on July 2007.

Leinfelden-Echterdingen 09/14/2007

Ads-tec GmbH

i.A.
Elmar Bossler
- Quality Manager -

i.V.
Dipl. Ing. Thomas Mögerle
- Technical Director

© ads-tec GmbH • Raiffeisenstr.14 • 70771 Leinfelden-Echterdingen

IF1110

Declaration of Conformity / Manufacturer Statement

●PRODUCT

NAME: Industrial Firewall
DESCRIPTION: Firewall
MODEL: DVG-IF1110-001-BU

● MANUFACTURER

ads-tec GmbH
Raiffeisenstr. 14
70771 Leinfelden-Echterdingen
Germany

Tel.: +49 / 711 / 458940
Fax: +49 / 711 / 45894994

● LAWS

EU Council Directive of 3 May 1989 on the approximation of the laws of the Member States relating to Electromagnetic Compatibility (EMC_Directive)

EU-Directive: 89/336/EWG from 5/3/1989 (ABl.EU L No. 139/19)
91/263/EWG from 4/29/1991 (ABl.EU L No. 128/1)
92/31/EWG from 4/28/1992 (ABl.EU L No. 126/11)
93/68/EWG from 7/22/1993 (ABl.EU L No. 220/1)

Adopted in Germany by: EMVG from 9/18/1998 (BGBl I 1998, 2882)

COUNCIL DIRECTIVE of 19 February 1973 on the harmonization of the laws of Member States relating to electrical equipment designed for use within certain voltage limits (LVD-Directive)

EU-Directive: (LVD) 2006/95/EC from 12/27/2006 (OJEU, L 374, page 10-19)
93/68/EWG from 7/22/1993 (ABl.EG L Nr. 220/1)

Adopted in Germany by: 1. GPSGV from 7/11/1979 (BGBl I 1979, 629)

● HARMONISED STANDARDS FOR TESTING

EMC-Directive

a) Electromagnetic emissions
EN 61000-6-4:2001

b) Electromagnetic Immunity
EN 61000-6-2:2005

LVD-Directive

Safety of information technology equipment
EN 60950-1:2001

● STATEMENT

The manufacturer hereby declares product conformity with the fundamental requirements given by the above-described directives of the European Union. The tests applicable according to the harmonized standards mentioned above have been fulfilled.
The CE labeling was assigned on July 2007.

Leinfelden-Echterdingen 09/14/2007

Ads-tec GmbH

i.V.

Elmar Bossler
- Quality Manager -

Dipl. Ing. Thomas Mögerle
- Technical Director